NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA

THESIS

INFORMATION WARFARE:
IMPLICATIONS FOR FORGING THE TOOLS

by

Roger Dean Thrasher

June 1996

Co-Advisors: Dan C. Boger
Carl R. Jones

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE	Form approved OMB No. 0704-188

1. AGENCY USE ONLY (*Leave Blank*)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	June 1996	Master's Thesis

4. TITLE AND SUBTITLE
INFORMATION WARFARE: IMPLICATIONS FOR FORGING THE TOOLS (U)

5. FUNDING NUMBERS

6. AUTHOR(S)
Thrasher, Roger D.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
USAF Institute for National Security Studies
USAFA/DFE
2354 Fairchild Dr., Suite 5D33
USAF Academy, CO 80840

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

One part of the modern Revolution in Military Affairs (RMA) is the possibility of a new form of warfare—often called information warfare. Development of information warfare depends on technological advances, systems development and adaptation of operational approaches and organizational structures. This thesis assesses the implications of information warfare for the technology and systems development areas, with the underlying motivation of ensuring the military is postured to "win the information warfare RMA" through effective research, development and acquisition. This assessment takes place primarily through a "Delphi" process designed to generate discussion between selected information warfare experts about the impacts of information warfare. This thesis concludes that information warfare is largely dependent on commercial information technology. This dependence means the military should rely on the commercial sector for most technological advances and products—with government research funds focused on military-unique research areas. Use of commercial items, coupled with DoD standard architectures, may enable a decentralization of information warfare acquisition to the user level. Finally, this dependence means the acquisition system should focus on architecture development, technology insertion, systems integration and on managing functions and services of systems—primarily through development of operational software to run on mostly commercial hardware.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Information Warfare, Revolution in Military Affairs, Research and Development, Systems Acquisition, Information Technology, Delphi, IW, RMA, IT	160
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF THIS ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std 239-18

Approved for public release; distribution is unlimited

INFORMATION WARFARE: IMPLICATIONS FOR FORGING THE TOOLS

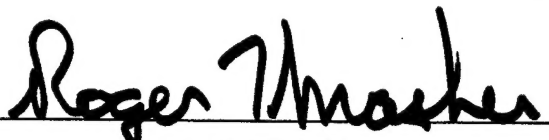
Roger D. Thrasher
Captain, United States Air Force
B.S., United States Air Force Academy, 1986

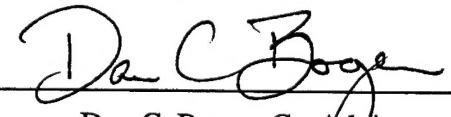
Submitted in partial fulfillment of
requirements for the degree of

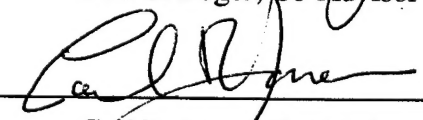
MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY (COMMAND, CONTROL AND COMMUNICATIONS SYSTEMS)

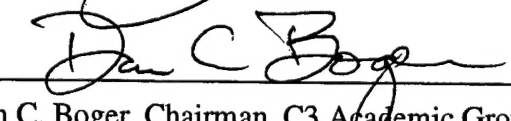
from the

NAVAL POSTGRADUATE SCHOOL
June 1996

Author: 
Roger D. Thrasher

Approved by: 
Dan C. Boger, Co-Advisor


Carl R. Jones, Co-Advisor


Dan C. Boger, Chairman, C3 Academic Group

ABSTRACT

One part of the modern Revolution in Military Affairs (RMA) is the possibility of a new form of warfare—often called information warfare. Development of information warfare depends on technological advances, systems development and adaptation of operational approaches and organizational structures. This thesis assesses the implications of information warfare for the technology and systems development areas, with the underlying motivation of ensuring the military is postured to "win the information warfare RMA" through effective research, development and acquisition. This assessment takes place primarily through a "Delphi" process designed to generate discussion between selected information warfare experts about the impacts of information warfare. This thesis concludes that information warfare is largely dependent on commercial information technology. This dependence means the military should rely on the commercial sector for most technological advances and products—with government research funds focused on military-unique research areas. Use of commercial items, coupled with DoD standard architectures, may enable a decentralization of information warfare acquisition to the user level. Finally, this dependence means the acquisition system should focus on architecture development, technology insertion, systems integration and on managing functions and services of systems—primarily through development of operational software to run on mostly commercial hardware.

TABLE OF CONTENTS

ACKNOWLEDGMENTS

The author would like to thank the USAF Institute for National Security Studies (INSS), Colonel David Todd, and Captain Mike McCarthy for their thesis sponsorship and financial support of thesis research travel. The author also wishes to thank the members of the Delphi for their participation and generous giving of their thoughts and time, LT Don Elam for sharing his own information warfare ideas and research, and Professors Dan Boger and Carl Jones for their insights and guidance. Finally, many thanks to Valerie, Rory and Carl Thrasher for their patience and understanding during this effort.

EXECUTIVE SUMMARY

Today, many feel that the world is in the midst of a Revolution in Military Affairs (RMA). The changes behind this RMA consist primarily of advances in information technology, which in turn enable gains in the precision, range and lethality of conventional weapons. But beyond enhancing how war was conducted in the past, many argue that a new form of warfare—called information warfare—is now possible. As part of an RMA, development of information warfare depends on technological changes, systems development and the adaptation of operational approaches and organizational structures in order to take advantage of this new capability. In terms of information warfare, much of the focus has been on assessing the operational and organizational issues. Less attention has been paid to the impacts on research and acquisition activities. Thus the focus of this thesis is on examining the nature of information warfare and the implications of the defining characteristics of information warfare for the research and acquisition systems.

Modern information warfare is heavily based on the use of information technology. With such use comes dependency, that in turn creates vulnerabilities that may be attacked and must be defended. The process of attacking an enemy's information and information technology vulnerabilities for any political or military purpose and the protection of one's own information and information technology is the essence of information warfare. The nature of information warfare is further delineated by the qualities of information technology itself:

- Has its own rules and limitations based on the unique traits of information technology
- No cleanly segregable systems in the traditional sense—more like C4I systems
- Dependent on commercial technologies available to most anyone
- Any warfare edge largely based on effective integration and exploitation of technology

These characteristics of lead to an investigation of whether the nature of information warfare will have specific impacts on technology research and acquisition activities.

Similar to the steps of a generic RMA, the impact of information warfare on acquisition can be probed by examining three different areas: technology, organization, and process. In terms of technology development, sowing the seeds for tomorrow's information warfare technology will require that the military engage with the commercial sector for the technologies to satisfy a large portion of military needs. Then the military would be free to spend its own limited funds on "investments in the margins" to address requirements not met by commercial developments. Some information technology characteristics may also make possible changes in the organizational structure of how such systems or services are acquired. One may be able to move to a decentralized system where users determine their own requirements and then local information technologists are largely free to buy, install and support their own equipment and services to meet their own user's information warfare needs. Promoting activities that enable this type of decentralization may be a key role of the acquisition world. Such activities would include continuation of R&D for military-unique issues, support for development of standards and architectures, development of contract purchase vehicles and demonstration of new technologies as a way to educate users. The organization to do this may not be that structurally different from today, although it might be greatly simplified and streamlined. Instead, it may promote ad

hoc alliances to address specific needs or collaborate on individual programs using modern information technologies. In terms of acquisition process, moves should be made to an incremental acquisition approach to keep up with advancing technology. There should be continual cycles of technology insertion via test beds and technology demonstrations such that the underlying system is never procured and disposed of in the traditional manner. With this goes an emphasis on managing the more stable functions that make up systems and on the information services required by the user. In many cases these functions will be embodied in mission-unique software and thus a prime focus of the acquisition process should be on development of operational software and integration of mostly commercial systems. In addition, the promise exists of cases where it may be cheaper and more effective to lease information technology or to discard an obsolete information appliance at the end of its useful life. Last is the issue of how to promote product integrity during design and development. To protect systems from information warfare risks, it will be important to ensure the systems engineering process includes activities that assess critical areas and that take steps to mitigate information warfare threats to critical system functions.

In sum, the defining characteristics of information warfare do prompt the need for changes in the acquisition community. Changes that range from focusing R&D on military-unique technologies useful in information warfare to organizational modifications in information technology acquisition to adjustments and improvements in the acquisition process. Changes that are key to ensuring the U.S. has the best chance of realizing the full promise of information warfare.

I. INTRODUCTION

> Victory smiles upon those who anticipate changes in the character of war. Not upon those who wait to adapt themselves after the changes occur.
>
> — Italian Air Marshall Guilio Douhet

Ever since the dawn of time when an unknown hominid first took up a tree branch (a tool) and smote his fellow hominid, warfare and tools have been inextricably linked. But the tools of warfare are no longer tree branches. With each new jump in tool-making (technology), often comes a matching increase in warfare capabilities. In a litany familiar to those who study such subjects, tree branches gave way to obsidian-tipped spears, copper swords yielded to iron swords, suits of armor to gunpowder-driven projectiles, and so on. Such progress has continued to recent times with the introduction of aircraft, combustion-engine vehicles, thermonuclear devices and the microchip. And sometimes the exploitation, development and fielding of these major technological advances have also enabled elemental changes or revolutions in the conduct of military affairs during a given age.

A. INFORMATION WARFARE REVOLUTION

Today, many[1] feel that the world is on the leading edge of one of these periodic changes in the fundamental conduct of war—that we are in the midst of a so-called Military-Technological Revolution (MTR) which may be causing a Revolution in Military

[1]Including Dr. Andrew Marshall of the DoD's Office of Net Assessment and several Russian military leaders (Kraus, September 1995).

Affairs[2] (RMA). The technological changes underpinning this modern RMA consist primarily of the stunning advances in electronic and information technology, which in turn are complemented by gains in the precision, range and lethality of conventional weapons (Krepinevich, Summer 1994). But beyond merely enhancing how we have conducted war in the past, many argue that a new form of warfare—often called information warfare—is now possible.

As the military moves into information warfare, advances in electronic and information technology are only the first step in fulfilling an information warfare RMA. Such military revolutions can be considered to have four primary elements, each of which must occur in order to achieve an RMA. These elements are:

- Technological Change
- Systems Development
- Operational Innovation
- Organizational Adaptation

(Krepinevich, Fall 1994)

Thus new technology can lead to the development, acquisition and fielding of new weapons, which in conjunction with new operational and organizational concepts of war, can result in basic changes in the conduct of war (Barnett). For the information warfare revolution, much of the focus has rightly been on assessing the doctrinal, operational and organizational issues. But less attention has been paid to the specific impacts of information warfare on technology research and acquisition activities. Given the ongoing clamor about the inadequacy of DoD acquisition and the continual call for acquisition reform, one must wonder if the research and acquisition systems are correctly postured to "win the IW RMA"

[2]See Andrew F. Krepinevich in "Cavalry to Computer, The Pattern of Military Revolutions," *The National Interest*, Fall 1994, for a good sketch of previous revolutions in military affairs.

(Christian, et al., May 1995)? Since if information warfare capabilities cannot be effectively[3] researched, developed and acquired, the U.S. may not realize the full potential of the information warfare RMA or completely develop its information warfare capabilities.

In order to ensure the U.S. does "win" the IW RMA, a group of Air Command and Staff College students have called for a revolution in acquisition affairs to "keep pace with the current information revolution and the IW RMA." Similar to the steps listed above for a revolution in military affairs, a revolution in acquisition affairs would consist of progress in three different areas: technology, organization, and doctrine (policy and/or process). This thesis will explore some of the issues in these three areas in an attempt to investigate the implications for acquisition affairs as a key part of the information warfare revolution in military affairs. (Christian, et al., May 1995)

B. RESEARCH FOCUS

As mentioned above, the primary research focus of this thesis is on examining the impacts of information warfare on the acquisition system. To further guide this investigation, a series of subsidiary research questions have been formulated. The first three questions are designed to provide background on the nature of information warfare and context for the remaining questions. The last three questions specifically probe aspects of the impact of information warfare on acquisition affairs. The specific subsidiary questions are:

[3]What is "effective" development relates to how quickly and cheaply one can put a suitable and operationally useful system in the hands of the warfighter. But it is also tied to how well one does development in relation to potential opponents.

- What are the characteristics of information warfare?
- What are the technologies of information warfare?
- What are implications of dependence on commercial information technologies?
- What are the future technologies of information warfare and how should research be directed to support information warfare?
- What organizational changes might be required in the acquisition community?
- What changes might be required in the acquisition process?

C. METHODOLOGY

This thesis will consist of a discovery and examination of information warfare acquisition issues. This discovery will primarily take place through the use of a modified Delphi[4] discussion, along with personal interviews with information warfare experts and through examination of literature in disciplines bearing on information warfare issues.

1. Information Warfare Delphi

The purpose of the Delphi conducted in support of this research is to facilitate a discussion on the impact of information warfare on the development and acquisition of DoD information warfare capabilities. This particular Delphi was somewhat modified from the typical Delphi methodology. First, interaction among the participants occurred only via electronic mail. This was done primarily because it enabled a very diverse group of individuals to participate in the Delphi effort independent of normal time and location considerations. While more convenient for the participants, this approach also has the

[4]The Delphi method is a research technique originally developed by the RAND Corporation as a structured way to bring together a group of experts to examine and brainstorm on a particular issue (Linstone, 1975).

drawback of not being very interactive. Second, unlike a more standard Delphi, there was no attempt to drive participants to consensus on any given issue. The purpose was more to elicit a wide range of responses and ideas—not to develop a single answer. There was also no ranking or scoring of responses and no statistical analysis of the inputs. Thus this approach may more correctly be termed a "multi-party interview" or perhaps a "Delphic" approach. But for the sake of clarity and brevity, this particular modified application of the Delphi research technique will be referred to as the "Information Warfare Delphi."

a. Participants

Delphi participants came from a variety of backgrounds, although each has some interest or expertise in information warfare. The group included active duty military members, DoD civilians, authors and corporate officials. The individuals[5] shown in Table I participated as members of the Delphi.

[5]Ranks, organizations and positions are current as of when the Delphi was conducted.

Name	Organization	Remarks
Col. (Ret.) Al Campen	Manager, AFCEA International Press	editor of *The First Information War*
VAdm Arthur Cebrowski, USN	Joint Staff	Director, J-6
Peter Cochrane	British Telecom	Director, British Telecom Research Lab
Dr. Fred Cohen	Management Analytics	author of *Protection and Security on the Information Superhighway*
James Dunnigan	Author	author of *Digital Soldiers*
LCDR(N) Robert Garigue	Director Intelligence, Security and Operations Automation, Canada	Deputy Program Director, Joint and Strategic Information Systems
Dr. Fred Giessler	National Defense University	Information Warfare Course Director
BG David Gust, USA	US Army	Program Executive Officer, Intelligence and Electronic Warfare
James Hazlett	SAIC	Senior Analyst
Ken King	Digital Equipment Corporation	Director, External Research Group
Dr. Fred Levien	Naval Postgraduate School	Chairperson, Information Warfare Academic Group
Dr. Martin Libicki	National Defense University	author of *What is Information Warfare?*
CDR Michael Loescher, USN	Office of Deputy Assistant Secretary of the Navy (C4I/IW)	Director, Information Warfare
Larry Merritt	Air Force Information Warfare Center	Technical Director
Dr. David Probst	Concordia University	Professor of Computer Science
Winn Schwartau	Interpact	author of *Information Warfare: Chaos on the Electronic Superhighway*
Robert Steele	Open Source Solutions	CEO
Col. David Todd, USAF	USAF/XOXT	Chief of Technical Plans

Table I. Delphi Participants

b. Approach

Three rounds of exchanges between the participants were conducted. Each round started with the presentation of the round topics created by the moderator. Each individual then sent their responses back to the moderator, who compiled all the replies and transmitted the consolidated responses to each participant for their review and further comment (if desired). Note that participants had complete freedom to address only those questions they were interested in or felt comfortable answering. Round topics were designed to match the subsidiary research questions and included more detailed issues and questions that will be discussed further in later chapters.

c. Synthesis of Results

The raw responses to the Delphi discussion were examined, common threads were extracted and serious differences highlighted. Then additional commentary was added as necessary to bring in other issues and considerations, as well as to draw conclusions from the author's viewpoint.

2. Personal Interviews

Personal interviews were conducted with several organizations and individuals involved in information warfare. In particular, interviews were held with Col. Ken Allard

of the National Defense University, CDR Mike Loescher of the Office of the Deputy Assistant Secretary of the Navy for C4I/IW, Capt. Mike McCarthy of HQ USAF/INXI, members of Rome Lab's information warfare team, and the Air Force Electronic Systems Center's information warfare program office.

3. Literature Review

Both official government and existing open source literature on information warfare was studied for applicability to this thesis. In addition, material on topics related to the various aspects of information warfare were consulted as required. Periodicals, books, briefs and papers examined are shown in the attached list of references.

D. ORGANIZATION OF THE THESIS

Chapters II, III and IV cover the first three subsidiary research questions and contain material designed to probe the general nature of information warfare, as well as several specific aspects of the technical nature of information warfare. These chapters set the stage and provide context for following chapters. Chapters V, VI and VII present the results for the last three research questions and move into an exploration of some of the possible technology, organization and policy implications of information warfare for the research, development and acquisition system. Chapter VIII concludes the thesis with a brief summary and some concluding thoughts.

II. CHARACTERISTICS OF INFORMATION WARFARE

The beginning of wisdom is calling things by their right names.

— Confucious

In the last few years Information Warfare has become a widely discussed topic within the Department of Defense and in the civilian world. But anytime you wish to have meaningful discussion on a particular issue, it is vital to have some common terms of reference. Such terms serve as a lingua franca and provide a convenient way to converse using shared concepts. Without such terms, communication is often difficult and consensus even more problematic. Such is the situation with information warfare. Although most everyone uses the term and many have proposed (differing) definitions for information warfare, there is little agreement about the specifics of the term. Alternative terms[1] such as cyberwar, netwar, information-based war, knowledge-based war, command and control warfare, information age war, etc., while possibly more precise, have not yet caught on in general use. So it has proven difficult to settle on one technically, doctrinally, and politically correct definition for information warfare. Instead it may be useful to approach the issue obliquely by discussing the unique aspects of information warfare by collecting observations from diverse viewpoints. Thus this chapter attempts to uncover the key

[1]The proliferation of alternative terms is itself troublesome and is reminiscent of the expansion of C^2 (Command & Control) to C^3 (Command, Control & Communications) to C^3I (Command, Control, Communications & Intelligence) to C^4I (Command, Control, Communications, Computers & Intelligence) to C^xI^y. In an article titled "C^1 Catharsis", Greg Todd makes light of this by referring to "$C^{27}E$: command, control, communications, computers, cohesion, counterintelligence, cryptanalysis, conformance, collaboration, conceptualization, correspondence, camaraderie, commissaries, camouflage, calculators, cannon, caissons, canteens, canoes, catapults, carpetbaggers, caddies, carabineers, carrier pigeons, corn whiskey, camp followers, calamine lotion, etc." (Todd, 1986)

features of information warfare and will serve as a basis of reference for discussions in future chapters. To address this issue, a series of four questions were put to the Delphi participants. These questions were designed to draw out opinions about the essential nature of information war, while at the same time avoiding hair-splitting discussions or rote regurgitation of various official definitions.

A. DEFINING CHARACTERISTICS

The first question asks about the defining characteristics of information warfare. While perhaps a deceptively simple query, the underlying purpose was to elicit discussion on the unique factors of information warfare. What makes this type of warfare different from, say, the characteristics of maneuver warfare or attrition warfare?

1. Delphi Responses

[Moderator] What are the defining characteristics of information warfare?

[Campen] The risk in seeking a definition is the temptation to look for correlation with the past, rather than defining differences. I have seen definitions of IW [Information Warfare] that are useless because they encompass all human endeavor. I argue that the definition of IW must be severely circumscribed if it is to be useful in assessing the impact on policy, doctrine, functions and organization on civil or military. We must seek out what is different from the past. I submit that difference is dependency upon vulnerable electronic technology. I limit IW to information (data) in electronic form and the hardware and software by which it is created, modified, stored, processed and moved about. The defining characteristics are dependency upon and vulnerability of electronic information systems. Example: Psyops [Psychological Operations] conducted via printed leaflets is not IW, but radio broadcasts or the electronic manipulation of TV images is. The physical destruction of a telephone exchange is not IW (telegraph lines were cut in the Civil War and submarine cables in WW One), but disabling a switch with a virus is IW.

[Cebrowski] The underlying character of information warfare is the proliferation of information-based technologies and their associated impact on society and by extension, on the bedrock issues of national security in the modern age. In warfighting, information-based technologies transcend the target sets of information, information-based processes, and information systems.

[Cochrane] The defining characteristic in information warfare is when information (in ANY form, so that includes ideas and philosophies) is supplied, or obstructed, with the aim of causing the information user to make a bad decision, or to confuse/overload their communication or decision making processes.

Examples:
- Knowing what your enemy does not
- Confusing the enemy with false information
- Damaging the information capability access of the opponent or denying him access to his own information
    - jamming of communications
    - hacking computer systems and changing or deleting data
- Interception of communications
- Use of disinformation
    - propaganda
    - cultural infiltration

[Cohen] The broadest common definition I have been able to get together is: Conflict in which information or information technology is the weapon, the target, the objective, or the method. From now on, I will use IT to indicate "information or information technology."

[Dunnigan] Attacking and defending the ability to transmit information.

[Garigue] The first thing that comes to mind is the realization that information warfare is a consequence of a new and emerging SocioTech structure. This emergence is not homogeneous throughout the world. Where as some Western societies are moving rapidly into it, others have not yet started. Modern societies are all presently engaged in building and riding a glass highway. With this in mind we have to face the fact that more and more of our social, economic, political and cultural transactions are digital in nature and all of them are computer mediated. Which means that in an information society no meaningful event can happen between individuals or organizations without computers and networks. We will have to fulfill our human interactions and commitments through our computerized social networks. We presently, and naively, place a lot of trust in these computer intermediaries that tell us the state of our complex systems. These systems may be cities, financial markets, health, wealth, production or even distribution. All these SocioTech systems are subject to computer control. Computerized networks bridge Decision Makers with an ever increasing array of sensors and effectors that monitor and intercede for us and help us in governing our complex environments. This trend will continue accelerating wherever efficiencies in systems can be found. As with a human constructed artifact there are flaws, failings and limitations. These new efficient networked SocioTech societies are also, and will always be flawed. Control over these systems is not more direct and local. Now it is remote and distributed. In open societies, authority to control is conferred by groups onto individuals via legitimate processes in accordance with common values and beliefs. But groups whose goals differ and whose objectives are at odds will try to impose control by force of arguments or might. So now in computer mediated societies as control has been somewhat centralized within the network layer, we see that there will be a clash of wills for control of that logical space. The fight for control of that space is called information warfare.

[Giessler] Competing and conflicting information, control and communication in complex adaptive systems—which all have teleological goals with the ultimate being survival...All systems are involved in information warfare—the only question is do they do anything about it? They can be a passive or active player. IW is all about decisions and the use of information, energy and material resources to offset disturbances that may drive your system away from the attainment of its objectives—especially the one about survival.

[Gust] Definition—after two years of discussion, the Army's TRADOC [Training and Doctrine Command] published FM 100-6, Information Operations. We argued and discussed the definition and who is in charge, even sought and rejected OSD [Office of the Secretary of Defense] staff advice on the definition. I do not believe there is universal agreement on it yet.

[Hazlett] Information Warfare is conflict between parties where information, or information systems are used to attack and defeat the enemy or when the enemy's use of, or access to, information is attacked.

[King] Information Warfare is a conflict between two parties where information technology is the primary means of obtaining a defensive or offensive advantage.

[Levien] One of the most critical of these is the fact that it is so imprecise. It obliterates any of the past definitional boundaries of "what is an act of war?", "what is war?", "who is the enemy?", "where or which is the enemies' territory or country of national origin?" This now much more difficult assessment of responsibility places new limits on how the military can react against a perceived threat to the country. In fact it becomes painfully difficult to determine an allowable course of action for a military officer to take when he (or she) is faced with the enormous body of U.S. law that (rightfully) limits and restricts those actions that the military can take against U.S. citizens. In today's world these same U.S. citizens are inextricably coupled via communications, business association, commercial activity, and just plain vanilla personal interactions with foreign (international?) entities...both friendly and often hostile as well. This can and most often does present a legal NIGHTMARE for the average military officer to sort out what actions he is permitted to take in this IW environment.

[Libicki] Information warfare is any activity motivated by the need to alter the information streams going to the other side and protect one's own. These range from physical and radio-electronic attack on both systems and sensors (or associated support systems), to cryptography, attacks on computers, and psychological operations.

[Loescher] What is new is that information creates and splinters the battle space, enables and defines the killing zone, and provides the means to execute the principles of war. I prefer to call this "war in the info age", which I think is a genuine revolution. In Navy, the term info warfare is being used evolutionarily by some communities to preserve and improve the past—better EW [Electronic Warfare], better cryptology, better, etc.

[Merritt] This is a good question. These days, there is a lot of press being given to equating IW to network attack (offensive and defensive). In my view, this is a very narrow interpretation and really is not doing the community justice in really working the problem. I think this is why we are now seeing more reference to other terms such as info dominance or info operations. In my view, IW consists of any action to exploit or affect an adversary's ability to gain a true picture of the battle space or to execute command and control of their forces. Also includes all the same activities associated with protecting our own capabilities. This truly brings in all aspects of EW, network attack, node analysis, intelligence, reconnaissance and surveillance, etc., both terrestrial and space based. This broad interpretation has been the cause of much controversy that has crossed traditional ricebowls and caused the community to concentrate on particular aspects of the problem.

[Probst] Information-based warfare is that branch of warfare information technology that supports two basic pillars of the Revolution in Military Affairs, viz., (i) Dominant Battlespace Knowledge, and (ii) Integrated Battlespace Management, including pre-engagement battlespace preparation, precision force (including just-in-time strike), and precision logistics. To be effective, these pillars require major advances in modelling and simulation, which in turn require (i) advanced control theory for automated full-spectrum strategic decision making, precision scheduling, and other information functions, and (ii) high-performance data assimilation and analysis for data-intensive predictive modelling and simulation.

Because it relies on high-performance computers and communications, Information-Based Warfare can be disrupted. Defensive Information Warfare tries to make sure that this cannot happen to our forces. Offensive Information Warfare—about which I have some reservations—tries to disrupt the computer-and-communications-based C4ISR [Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance] of the adversary.

Definitions aside, we can see three embryos of Warfare Information Technology today. These are:

- total situational awareness ==> Integrated Battlespace Management
- network security ==> Defensive Information Warfare
- the USAF Captain, using SIPRNET [Secret Internet Protocol Router Network], who subverted the Navy's Atlantic Fleet command in September 1995 ==> Offensive Information Warfare

The following is an equivalent vanilla base line for Information Warfare:

- high-performance information-based warfare with dominant battlespace knowledge, and precision force—including offensive information warfare—will alter the strategic, operational, and tactical levels of war (i.e., it will change the appearance of combat)
- information infrastructures are now part of the logistics tails of all armed forces, and—as such—require careful defense
- conversely, one may consider degrading the information systems that enhance the military capabilities of the adversary

[Schwartau] I maintain that True Information Warfare is the use of information and information systems as weapons against target information and information systems. I eliminate the call for or use of any bombs or bullets in True Info War. IW can attack individuals, organizations or nation-states (or spheres of influence) through a wide variety of techniques:

- Confidentiality compromise
- Integrity attacks
- Denial of Service
- Psyops
- Dis/mis-information, media, etc.

Most clearly, though, the distinctive feature of Pure IW is that it can so easily be waged against a civilian infrastructure in contrast to a military one. This is a new facet of war, where the target may well be the economic national security of an adversary. In addition, though, we have distributed capability to wage war. Today, a small band of antagonists can launch an IW offensive from behind their desks thousands of miles away; or a group of U.S. hackers might choose to declare war on another country, independent of any official U.S. sanction. The capabilities of IW is the issue: how much havoc can I rain without resorting to bombs and bullets. A lot is the answer, and I'm not the only smart guy on the planet.

[Steele] The defining characteristics of information are:
- Connectivity (all mediums)
- Content
- Coordination (standards, procurement)
- Communications & Computational security
- Context (both cultural and substantive)

Information "warfare" is almost moot or an oxymoron. In this era, failing to be competitive in optimizing the above five aspects of information is tantamount to abdication. At a very simplistic level information warfare can be thought of as an attack on any of the above five elements (e.g., denial of service or corruption of content). On the defensive side, again at a simplistic level, it can be considered in terms of continuity of operations. Unfortunately, our own DoD will never be a serious IW player until they figure out that collecting information, and the sensor to shooter interface, is the heart of information-based warfare operations.

[Todd] With warfare in the information age, our ability to control and exploit the information battlespace will be as much an enabling factor in combined warfare as the ability to control and exploit the air and space battlespace to enable conventional combined terrestrial warfare in the industrial age. Note that I don't use the term "information warfare." The challenge of warfare in the information age is more pervasive than the commonly thought of niches of information warfare. But within this category of IW falls our capabilities to attack an adversary's information function (regardless of means), the protection of our information functions (regardless of means), and that IW is a means, not an end.

2. Commonalities and Differences

First, it is clear that most Delphi participants agreed that much of the current ado about information warfare is related to the exploding capabilities of information technology. Rapidly expanding dependence on information technologies, both in society at large and in the military, is creating a situation where sometimes vulnerable information processing, flows and stores[2] can be attacked to gain military advantage. But here is where divergence starts to occur. Some felt that the focus should be on information technology itself as the method of information war. This case posits that only attacking your enemy with "non-physical" information technology-based methods constitutes true information warfare. Under this view, bombing an early warning radar would not be information war. While using malicious software to confuse the radar would be information war, even though the results in both instances might be the same.

Most participants, however, expanded the scope of information warfare to focus more generically on the concept of information itself. As historians are fond of pointing out, attacking an adversary's information functions is not really new and is not necessarily waged with information technologies. What is important is not the form in which the information is processed, stored or transmitted (it can be in a computer, in a brain or on a wax-sealed parchment), but somehow attacking the actual content of the information. Nor is it important how the information was attacked. Thus from this view dropping leaflets to impact the mind of a frontline Iraqi soldier would be considered information warfare just as much as high-tech radio broadcasts aimed at that same soldier.

---

[2]The term "information function" will be used to refer to information processes, flows and stores.

Implicit in all of this is the idea that we must protect our own information functions from exploitation and attack (commonly referred to as defensive information warfare). Most of the discussion in this area has been related to protecting our own networks and computer systems. Not much has been said about protecting information in other forms. For example, how should the U.S. protect its own frontline soldiers from propaganda?

Lastly, there were several unique views that merit further examination. One view is that information warfare constitutes any action which degrades the capability of the enemy commander's picture of the battle and prevents him from exercising effective command and control. This flavor of information warfare is called Command and Control Warfare (C2W) and has been initially designated as the military's battlefield implementation of information warfare (CJCS MOP 30, 1993). This is much more restrictive than the other definitions in that only the commander's information functions are targeted.

Another concept raised by one of the participants brings to mind the theory of reflexive control. Largely developed by the Russians, reflexive control involves the idea of trying to feed information to influence an opponent to voluntarily reach a certain conclusion or decision that is helpful to one's own cause. At the same time, the opponent is trying to do something comparable to friendly forces. If one thinks of information warfare as dealing with such "competing cybernetic systems," then this combination of reflexive control systems would be a "subsystem of information war." (Giessler, July 1993)

A final perspective expressed is that information warfare is simply a result of a "new and emerging Sociotech structure." This structure is characterized by the use of information technology to facilitate the day-to-day transactions of society and by the use of information technology to track the status of complex social and economic systems. Power

and control in such a Sociotech structure would be more diffuse and distributed and would reside within the network layer. The fight for control of the Sociotech structure via the network would be called information warfare.

B. INFORMATION IN WAR VERSUS INFORMATION WAR

The next issue addressed by the Delphi group deals with the distinctions between the use of "information in war" and information warfare. What separates the two ideas? Are they really different? This question aims to further circumscribe information warfare by comparing and contrasting these two concepts.

1. Delphi Responses

[Moderator] Are "information in war" and information warfare the same?

[Campen] Definitely not. Information-in-war describes how information has been used since the dawn of conflict: Always sought, usually too late or wrong, not always properly used or effective when used. Information-in-war was serendipitous and usually incidental to the conflict. It was an adjunct to war, with an impact varying from nil to absolutely vital in rare, notable incidents. In IW, if there is no information there may well be no war. Example: Smart missiles but no means to instruct them, or the XXI [Force XXI] Soldier who's GPS [Global Positioning System] fails, is lost, and cannot perform assigned function, or "just-in-time" logistics that aren't.

[Cebrowski] No. The premise of information in war involves the process by which raw data (sensors or intel sources) is converted to information for decision-makers, and how that information is distributed and acted upon by operational commanders. Information warfare is the means by which we affect information in war. This can be done by targeting an adversary's information, information-based processes, information systems or computer-based networks. Equally important is protecting our own information, information-based processes, information systems, and computer-based networks.

[Cochrane] Information is a tool and a target of war (just like a tank or a munitions factory). Information in war includes details about the enemy (his strengths, weaknesses, deployment, location of resources, communications). Information warfare is using information technology, either to gain data about the enemy or to destroy the enemy's data resources or cultural support.

[Cohen] Not in my view. Information in war includes every aspect of IT as applied during conflict. IW includes only situations where IT is the weapon, target, objective, or method. For example, supporting warfighting with mapping and weather information is not IW except in the cases where the mapping information is the weapon, target, objective, or method of conflict. In ancillary roles, it's not part of IW. In this view, every piece of IT may sometimes be part of IW, but most parts are never part of IW. In other words, it is the "USE" of IT and not some inherent property of the IT that applies.

[Dunnigan] No. The former is a product, the latter is an action.

[Garigue] The distinction is akin to looking at the subject that performs the action or the object on which we act. These are different approaches to the same subject. Although many would see them as different I see them as being a continuum. From the meta-strategical aspects of Information Warfare we see what we are trying to achieve, such as looking at the objectives and the criteria by which we determine if we have achieved them or not. Information in war relates to the managerial aspects of how to do it. So Information Warfare help us to focus on effectiveness issues and Information in War helps us focus on efficiency issues. But the two cannot be separated from each other and need to be considered as a two sides of a same coin.

[Giessler] No—the DSB [Defense Science Board] concept from the '94 summer study was valuable. I in W is the use of information technologies to better conduct what we traditionally know as modern warfare and the Tofflers would call warfare in the industrial wave. In this mode information is a supporting element to air, land, sea, space and SOF [Special Operations Forces] warfare. It is a force multiplier. IW is warfare in the information realm, environment and age. It includes old but also new forms and qualities of warfare—the fight for survival. It is facilitated by IW technologies that create a unique confluence that allow competition and conflict never before considered. And we are about as smart about what that warfare is as Billy Mitchell was about air warfare and power in 1917 when he was teaching and thinking about it at Langley Field.

[Gust] Info in war can mean the Blue Force use of info while info warfare means, to me, both Blue Force protection actions of their info while offensively exploiting the Red Force's info.

[Hazlett] No, many forms of information are used in war, not all of which is used in information warfare. In information warfare, information is the weapon and/or the target.

[King] No. All participants in a war have always made use of any available information but it was always in support of the primary operations.

[Levien] "Information in war" and "information warfare" are poles apart in meaning. (Ah the beauty of the English language!) Information in war…is essentially a meaningless phrase in that it adds very little to the concept of the role information plays in wartime as opposed to any other time in the affairs of man. On the other hand…coining the new term "information warfare"…where information is the descriptive term of war…implies a new dimension of how to wage war, which is as highly distinct as the term (for example) Nuclear War. The potential effects of IW, while not as physically dramatic as nuclear, could nevertheless in the future be as historically significant as nuclear war in its resulting outcome.

[Libicki] Information in warfare is so broad a category as to be meaningless; what kind of warfare does not involve information?

[Loescher] See above.

[Merritt] I don't think so. Info in war as I see is that info that allows you execute your mission. This is needed in whatever conflict that we are involved in, whatever realm we are operating (i.e., space, air, land, info). Info war is the utilization of the info realm to gain advantage in wartime.

[Probst] Information In War has an elementary and an advanced stage. In the elementary stage, data is converted into information for use by experienced decision makers; in the advanced stage, viz., integrated battlespace management, computer systems generate and evaluate alternate warplanning scenarios using modelling and simulation technology.

Information Warfare concerns the protection or disruption of this process.

[Schwartau] Absolutely not. I consider information in war to be making conventional weapons more efficient; to bring better information to the HQ [Headquarters], process it better and faster, and get the necessary information out to the war fighter as fast as possible. The closer to real time and iterative the process is, the better. This approach makes wars less bloody, increases efficiency and maximizes the capabilities of the existing arsenals. What I find intriguing about this thought model is that is the same paradigm for commercial companies, except for the bullets, which makes it in their case closer to a Class II style information war.

- Market research
- Competitive analysis
- Decision making
- Sales/Marketing efforts
- Feedback

The convergence of military and commercial IW issues is obvious, at least to me. :-)

[Steele] See above. "Information in peace", or information peacekeeping, is the flip side. Where we have a major disconnect today is in the existing bureaucratic mind-sets and forms of organization. The battlefield is civil, but no civilian organization is ready to get organized, and the military is saying "it's not my job" to provide for the common defense of the civil sector...

[Todd] Military history has multiple examples of how "Information in war" is often the leveraging factor in successful engagements and campaigns. But the common thread is that engagements were necessary to impose one's will upon the enemy. At the other end of the pendulum, information warfare is viewed along the lines of Toffler and Schwartau in which one can impose one's will upon an adversary through the control, manipulation and denial of information, similar to the Soviet theory of "reflexive control." A more useful notion is that of information-based warfare. This falls in between those two extremes. Not only is the advantages of information technology realized through the abilities to engage the adversary with less friendly forces but having overwhelming impact due to timing and targeting, but in information-based warfare we can integrate military disciplines to manipulate the adversary's perceptions at the tactical, operational

and strategic levels. Information-based warfare, consistent with previously accepted operational art, will still require changes in organization, technology adaptation, and changes in operational concepts and doctrine.

2. Commonalities and Differences

There was clear consensus that "information in war" and information warfare are not the same—although both may make use of information technologies. Better "information in war" can be used to enhance conventional warfare tasks such as movement, fixing, command & control, targeting, striking, logistics, etc. Under this view, using a computer to automate resupply of tank parts is not information warfare but is improved logistics. Nor are the F-22 or Comanche information warfare platforms no matter how many microprocessors are in them. It is the purpose for which we use information technology and not just the simple use of information technology that defines whether it is "information in war" or information warfare. The use of information to enhance our own operations is thus different from protecting our information functions or attacking our adversary's information functions (the latter two activities constitute information war). Admiral Cebrowski sums up the group's thinking very nicely when he states that "information warfare is the means by which we affect information in war."

C. REFLECTIONS ON CYBERSPACE

There is much talk about "cyberspace" or the "infosphere" in discussions about information warfare. Many contend cyberspace is a new realm of struggle and contention on a co-equal status with the more traditional realms of air, land, sea and space. This question attempts to explore whether cyberspace is in fact a new domain of warfare.

1. Delphi Responses

[Moderator] Is "cyberspace" a new medium (like the traditional media of air, land, sea and space) of competition and conflict between nations, businesses and other organizations?

[Campen] No. Land, sea, air (and perhaps space someday) are media where physical things (people, ships and aircraft) interact. If cyberspace means the ether, then it does not qualify because no conflict actually takes places in that media. If cyberspace is defined as including the physical devices mentioned above (computers, communications, etc.), then it does not qualify because those devices are being employed in one or more of the existing media (air, land, sea), not in the ether.

[Cebrowski] Cyberspace is more of a cliche than a medium. A medium implies that definitive boundaries or characteristics exist—cyberspace is too ubiquitous to be bounded, and thus, shouldn't be considered a medium.

[Cochrane] Information is a commodity of war, like food and fuel. Cyberspace is a new transport mechanism and hence a target like a road. Cyberspace covers sea, land and air with its transport mechanisms. The fact that the Internet is accessible by anyone from anywhere in the world means that machines attached to the net are under threat of attack from unfriendly machines which are also connected.

[Cohen] New? Not really. Separate and different? It may be advantageous to treat it that way.

[Dunnigan] Only new in terms of much greater mass and velocity.

[Garigue] Cyberspace is not a physical space but a true social space. Unlike the other mediums where geography and physics structures relationships of force, in Cyberspace only information and knowledge determines the structure of power. Distances, geography, and borders become artificial and abstract notions and do not regulate the relationships between individuals and organizations. There are no inherent constraints in Cyberspace (except bandwidth and IP [Internet Protocol] addresses but this is not seen as a major source of future conflict) so there is no real reason to fight for possession of something that has no space or territory. However, the fact that this domain can amplify perspectives and thus exert influence over Decision Makers as well as potentially control systems that can acquire, transmit, store, analyze and produce wealth, there is certainly a danger of a clash of goals.

[Giessler] It is a new realm of conflict and competition that has evolved since the mid 1800s. But the advent of the chip, satellite coms and sensing, fiber optics and technological advances in software, hardware, orgware, brainware, decisionware, etc. have created changes which have resulted in a discontinuous function and reality.

[Gust] Cyberspace, like frequency spectrum, will become a nationally controlled asset. Due to access via various means, i.e., direct satellite, phone lines over land, fiber optic cables undersea, etc., it will be hard to control. Use now precedes policy.

[Hazlett] Yes, it has boundaries similar to those between other mediums and environments, across which attacks can be mounted either physically or electronically.

[King] "Cyberspace" is a new medium of communications with its own set of characteristics. Commerce will become the primary medium of competition and conflict and the most likely target of electronic attacks.

[Levien] Cyberspace is a concept of a state that exists only in the mind's eye. It has no physical properties, no dimensions...nothing to touch...or feel. This as opposed to land, sea, atmosphere, etc., which can be described with physical constants and dimensions and to which the Laws of Physics (immutable as they are) can be applied thus allowing us to predict their behavior. Not possible with Cyberspace. So if you can't describe it...and you can't predict it, it's hard to protect yourself from it. You can perhaps try to change the effects which it produces, but that is another matter altogether.

[Libicki] Unlike all other media, there is no such thing as forced entry in cyberspace.

[Loescher] Potentially. But Clausewitz has to be reexamined in our age. War is only an extension of politics if there is a discernable politic. I don't think the medium is inherently a medium of competition and conflict. But it probably will become so like the others. It's probably better to think of information as a competitive topic than of cyberspace this way—although cyberspace is definitely a new medium the prime characteristics of which are virtuality (i.e., independent of time and space)

[Merritt] In my view, yes. Many contend it is nothing new but just an extension of old capabilities. I disagree. The ability to quickly gain access to data, systems, etc., anywhere in the world within seconds is a leap of capability that is just now being utilized. In my view, we have barely scratched the surface of this capability. In this "virtual world" a whole new methodology with new tactics, new laws, new players, and new results tends to support the argument that this is indeed new and until we get true buy-in on this issue, the true capabilities of IW will not be realized.

[Probst] If it is possible to attack across cyberspace, and to achieve cyberspace dominance, then we would have to call it a new medium. I think this is an exaggeration. What is feasible is to have an order-of-magnitude competitive advantage in both battlespace knowledge—which implies understanding—and integrated battlespace management. Your question then becomes secondary.

[Schwartau] Hell yes! If I have the ability to raise havoc with an Army or Navy or Air Force, and I exclusively use cyber-weapons, then of course it's an added dimension. The weapons arsenals I propose use:

- *invisibility*
- *passivity*
- *insidiousness*
- *mind screwing*

I believe we need a center of IW excellence, yes, perhaps an independent force, which houses all of the expertise, and then is appropriately distributed as needed to other services as required. This "Cyber-Force" (I don't have a better name yet) can act on it's own without conventional service aid, or in combinations with others.

[Steele] An old medium with a new importance. Especially troubling because of the stealth and anonymity that any individual can exploit. Has radically altered the balance of power between nations, organizations, and individuals, and left all intelligence communities two decades behind the learning curve.

[Todd] "In many respects, one can consider information as a realm, just as land, sea, air, and space are realms." Realm as defined as: the region, sphere, or domain within which anything occurs, prevails, or dominates. "Information has its own characteristics of motion, mass, and topography, just as air, space sea and have their own distinct characteristics. There are strong conceptual parallels between conceiving of air and information as realms." {Cornerstones of Information Warfare, Sep 95}. Just as air and space forces attempt to control and exploit air and space in order to enhance all military force's effectiveness, so to must all forces attempt to control and exploit the information realm to enhance all military force's effectiveness.

2. Commonalities and Differences

Three basic views about cyberspace seem to emerge from this discussion. The first is that cyberspace is not a new medium of competition and conflict. It is simply an artificial construct of the human mind that doesn't have definitive boundaries, has no physical existence separate from any of the existing media, and has no real governing laws akin to the laws of physics in the normal physical world.

Others took the exact opposite view, arguing that cyberspace is an old conflict realm that has gained new importance with the advent of advanced information technology. The growth of world-wide interconnected information systems and sensors has led to the birth of a "social space" which is distinguished by being independent of time and physical boundaries, by the ever increasing amount and velocity of information, and governed by the peculiar rules[3] and protocols of digital technology. This viewpoint has much in common with the development of air warfare. Much as aerial technologies allowed one to exploit the realm of the air (which had always existed), information technologies allow one

[3]One facet of which is what Dr. Martin Libicki was talking about when he said "there is no such thing as forced entry in cyberspace." Unlike targets in the physical media, you cannot forcibly "take" a computer system in cyberspace unless there has been poor systems design or systems administration.

to exploit a cyberspace that has always existed, even if it hasn't been formally recognized as such.

Finally, there was the view that cyberspace is really more of a transport mechanism than anything else. Much like a road system or the frequency spectrum, use of cyberspace to transport and store information will make it a natural target in war.

In the end, no consensus was reached. What is clear is that the conditions often associated with cyberspace, and therefore the rules under which information warfare is conducted, can differ greatly from conflict in the traditional realms of war.

D. NOTHING NEW UNDER THE SUN?

King Solomon once said, "There is no new thing under the sun." Many skeptics and agnostics say the same thing about information warfare. This proposition was put to the Delphi participants in an attempt to draw out what is novel about information warfare and why there has been such a surge of interest in information warfare.

1. Delphi Responses

[Moderator] Is there really anything new or different about information warfare?

[Campen] Definitely. Because of dependencies and vulnerabilities of information systems, the potential exists to gain advantage or victory without resort to traditional means of force, or perhaps with fewer forces. Example: Manipulation of opponent sensor data can make things appear other than they are. Manipulation of opponent data could disrupt logistics and troop flow. (Fustest with the mostest!) when you are actually neither.

[Cebrowski] Although the nature of war will always remain constant, the character of war is in constant change. Information permeates society—as a pillar of national security, as well as the military—where the fractional component of information technology continues to grow in warfighting systems. U.S. dependence on information and associated technologies, coupled with rapidly expanding global interdependencies, exposes vulnerabilities that can be exploited using IW, both here and abroad.

[Cochrane] One potential difference for countries like the U.S. is that the battle can be waged with the civilian population in their own backyard from day 1. In this respect information warfare could represent a threat that is comparable to nuclear missiles, without the tell-tale sign of a missile launch.

Important factors are:
- Low entry barriers mean ANYONE can start a "war"
- The speed of distribution
- More numerous ways of going about the war
- Harder to find the culprits
- More efficient (bigger bangs for your buck!!!)
- A success will be seen by more of your enemies
- Inflicted damage can potentially be far higher than earlier technologies

[Cohen] Yes. The difference is that we now depend on IT for every aspect of our existence as a society. This increased dependency means that the inherent vulnerabilities of IT extends to our ability to wage war, survive economically, and to the very fabric of our society.

[Dunnigan] Greater mass and velocity. U.S. Grant standing next to a telegraph operator was waging info war, but the speed of data transmission was less than 300 baud.

[Garigue] Yes—but most of it has yet to be seen as the impact of living in an information society becomes real. However, the initial impact will be the rapid redistribution of power away from institutions that used to control simply through possession of information; such as intelligence organizations, government, big corporations, multinationals, and professional organizations. Power will come from the capacity to create and apply new knowledge. It is the capacity to apply new knowledge that will permit organizations to determine their future by simply deciding which future they want.

[Giessler] Yes—much is new. The newest is that we don't know what all is new. Just as Billy [Mitchell] didn't know how air warfare was new we are incapable of specifying how IW is new. And it doesn't make any big difference. Those who can not allow out-of-the-box thinking will just not survive in the info age. They may be fine if they stay in the industrial age. They will even be needed there. IW is all about influencing minds (as Sun Tsu wrote about) but with new technologies and wares.

[Gust] We have some thinking to do about jamming vs. intercept. We can now do so much more selective jamming and denial, and destruction because of technology. Intercept still provides so much Red Force intent that it must not be set aside because of our ability to defeat the Red info systems.

[Hazlett] Yes, in information warfare, information is the target, and sometimes the weapon. In other forms of warfare, it is generally a bi-product or collateral target, but not the primary medium or target.

[King] It is different in that the experience and expertise from centuries of regular warfare are of very little value in information warfare. Thus it is a revolutionary change not an evolutionary one.

[Levien] To answer this question you have to decide what your timeline of reference is for the word "NEW." When do you start in deciding what is new? In many ways IW is simply a repackaging of a great body of knowledge that has been around for quite some time. PSYOPS, deception, for example...the world's history is replete with example after example of these two subjects. Ditto with the fifth "pillar" of C2W destruction. As you get to the subject of EW in C2W, you have a more recent series of events to consider. But it is clear that unlike the dawn of the nuclear age, with the discovery that $e=mc^2$, there is no single defining technological breakthrough that heralded the age of Information Warfare. There ARE some technologies that make the advance of civilization possible which then in turn were applied to warfare (as always) but these were not specifically developed for Information War. What has happened is a sort of rearranging of the chairs around the table of knowledge. But this is not a trivial shift. For it opens up...no, rather it demands...that the military strategist and planner consider fields of interest which heretofore he has been (happily) able to almost ignore. The most significant change that I see occurring is:

IT REQUIRES A MUCH CLOSER COUPLING OF THE MILITARY AND DOD WITH THE U.S. INDUSTRIAL AND COMMERCIAL BASE IF WE ARE TO SURVIVE AS A NATION.

This relationship in the past has often not been a close or comfortable one, with both parties trying to keep the other at arms length. (With the possible exception at the height of large wars). And it certainly is not the general attitude of the U.S. populace at large these days with the desire to keep the Government more and more out of our daily lives. In the response to our efforts to combat the threat of IW, it may finally dawn on both sides of the parties to these debates, that closer ties are no longer an option. If one examines the actions of some of our "allies"...e.g., France, Israel, Japan...you can see these partnerships forming with often devastating results to U.S. interests.

[Libicki] At the operational level, as the processing of information becomes systematized (e.g., the systems component of the command center, Admiral Owens' System of Systems, the NII [National Information Infrastructure]), attacks on and defenses of such systems becomes important. At the strategic level, there is nothing really new.

[Loescher] Yes. See above.

[Merritt] See above. I think yes...

[Probst] There are two new aspects, both rather obvious. Progress in high-performance computers and communications will lead to a Revolution in Military Affairs, although there are more advanced and less advanced thinkers about how this should happen. We depend on our computers in unprecedented ways. As cooperation gives way to contention, we find our computers have much thinner skins than we ever imagined.

In brief,

- information technology is on the point of causing a paradigm shift in information-based warfare
- we may generalize counter-force to counter-information system

[Schwartau] I keep hearing the arguments that IW is nothing new, but I have to argue that for the first time in history, the capability exists to wage a conflict (indeed a war) where no conventional munitions are required to achieve a stated goal; be that goal isolation, economic deactivation, sanctions or alternative to combat.

[Steele] Not yet. All I see at this point is industrial age concepts applied very poorly to information age opportunities.

2. Commonalities and Differences

There was almost complete consensus on this question. Most participants felt that the modern incarnation of information warfare is something substantially new. The main reason for this thinking relates to the vastly increased use of information technology in society at large, as well as in the military. Such use implies a dependence on information technology and dependence results in vulnerabilities should the use of information technologies be denied or otherwise interfered with. Attacking (or protecting) the vulnerabilities created by information technology use is the basis of information warfare.

There are also some special aspects of these information technology vulnerabilities. First, the interconnected nature of information technology changes the frontlines of warfare. No longer is the United States immune to direct non-nuclear or non-terrorist attack of the continental homeland. Previously the only two realistic ways to directly attack the United States proper were to be a superpower with intercontinental ballistic missiles or to be a terrorist. The former takes immense resources and the latter typically has had only limited effect. Information warfare requires no such immense resources and has the

potential for widespread impact. This combination of direct attack with low entry cost and tremendous possible impact is new.

Another new aspect involves the speed with which information warfare may take place. Unlike current warfare means, information warfare by nature may require no obvious build-up or marshalling of forces. And when attacks do take place, the speed with which results may occur has the potential to be very quick.

Finally, from a more purely military standpoint, some participants stated that what is really unique is that information warfare gives commanders the promise of a new way to wage war. As the *Economist* states, "If information warfare means something new, it is the use of information as a substitute for traditional ways of fighting, rather than as an adjunct to them" (*Economist*, June 10, 1995). If this is true, then Mr. Ken King's statement that expertise in prior warfare does not translate to expertise in information warfare is a subject that bears further attention and study.

E. SYNTHESIS

Given the diversity of views expressed above, are there any common threads or integrating themes that can be drawn about information warfare? Although the Delphi participants in general rejected the notion that the use of "information in war" and information warfare are the same, the distinction is not so clear to others. For example, a recent article about an upgraded artillery fire control computer referred to it as an "information warfare system." Such discussions about the use of information and information technology in conflict and war have somewhat naturally led to the label of information warfare. The problem with this broad view is that almost every activity in war

requires information and would therefore be some form of information warfare. It is probably more precise to speak of information-enhanced warfare. In the information age, this involves the use of information technology to better accomplish normal warfare functions like command, control, move, find, fix, shoot, logistics, personnel management, etc. So "digitization of the battlefield," Dominant Battlespace Awareness and C4/ISR are not information warfare but information in war—even if they all indisputably entail information and information technology.

What then is left for information warfare? The key is in the new and growing dependence on information technology—both in the military and perhaps more importantly in society at large. One now may be able to target and attack the information functions of adversaries in ways that were not possible until the widespread adoption of information technology. Thus attacking an enemy's information and information technology vulnerabilities and protecting one's own are the essence[4] of information warfare. The new Joint Chiefs of Staff definition of information warfare takes this view:

> Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks. (NDU IBW Course Slides, March 1996)

The emphasis is on targeting enemy information functions while protecting one's own—but does not include one's own use of information or information technology for the enhancement of various warfare purposes. Also obvious is the prominence given to

[4]Deciding whether information warfare occurs in a "cyberspace" that is a co-equal realm with air, land, sea and space is probably not critical, as long as it is recognized that information warfare conflict has its own physical and logical rules and limitations that must be considered when conducting such warfare.

attacking and protecting information technologies such as information systems and computer networks.

One issue that remains is whether information warfare is also defined by the means used, by the target attacked or by the purpose for attacking the target. The JCS definition states that the purpose of information warfare is information superiority. So if one attacks a computer-controlled drawbridge with a virus for the purpose of "taking out" that bridge, is that considered information warfare? The purpose was clearly not information superiority, although many would still label this an information warfare attack because of the means used. Likewise, disabling a tank by disrupting its microprocessors with an electro-magnetic pulse could be considered a "strike" via information warfare means. Thus the sole emphasis on information superiority may be too exclusionary. While certainly information superiority is a major goal of information warfare, it can be argued that more traditional warfare purposes can also be served by attacks on vulnerable information technology. If one can disrupt the adversary's warfare functions (be it C2, strike, reconnaissance, logistics, etc.) via attacks on the information technology that he uses to support those functions, then information warfare becomes one more means (as is physical destruction) to a particular military end (like interdiction, C2W, anti-infrastructure, attrition, etc.). Likewise, if one can disrupt some of the adversary's social or economic functions via attacks on the information technology that he uses to support those functions, then information warfare becomes one means to a particular political or diplomatic end (like economic blockage, isolation, etc.).

In summary and at the risk of adding to the confusion of terms, one might break down the subjects of information and warfare into a simple taxonomy. At the top would be

"Information Age Warfare" or "Third Wave Warfare." These terms would be comprised of all the aspects of modern and near-future warfare. One of the main features of Information Age Warfare would be "Information-Enhanced Warfare." This term recognizes the revolutionary impact of information technology on all of the functions of war. Another separate facet would be the over-worked term of "Information Warfare" as the moniker for attacking an enemy's information functions while protecting one's own.

Is there now a better view of the essential elements of information warfare? The answer may be yes, but it is obvious that the full picture has not been revealed quite yet. The problem of overloading the term "information warfare" with different meanings still persists and is likely to for the immediate future.

III. TECHNOLOGY OF INFORMATION WARFARE

> The most signal contribution by Alfred Thayer Mahan in the field of military doctrine was his recognition that the conduct of war changes rapidly with technological advance.
>
> — Dale O. Smith

Dr. John Arquilla and Dr. David Ronfeldt argue that information warfare has been around since the time of Ghengis Khan (Arquilla and Ronfeldt, 1992). Why then all the recent attention? Much of the contemporary focus is related to one of the defining characteristics of information warfare identified in the last chapter—the stunning advances in information technology made in the last few decades. These advances are opening up new opportunities and avenues for information warfare. Since technology appears to play such an integral part in modern information warfare, this chapter seeks to explore the implications of this relationship through a series of questions put to the Delphi participants. These questions also set the stage for discussions of how to research and develop future information warfare technologies.

A. DEPENDENT OR ENABLED?

This question attempts to investigate whether technology is a requirement for waging effective information warfare or if technology is merely an amplifying factor. Does technology simply help to perform information warfare better or does information warfare depend on technology for its existence?

1. Delphi Responses

[Moderator] Is information warfare technology dependent or technology enabled?

[Campen] Both. Same coin, different sides. By above definition, IW is the child of technology and its greatest weakness and capability. If one side is overly enabled, it can become overly dependent and overly vulnerable.

[Cebrowski] Information warfare is more technology enabled since it focuses on the vulnerabilities and opportunities presented by the increasing dependence on information and information systems. However, other aspects of information warfare exist in part, outside the domain of technology—psychological operations and elements of intelligence for example.

[Cochrane] Technology simply enables new forms of information warfare to evolve but with similar target end points. You used to have to print lots of leaflets and fly your Sopwith Camel over the enemy lines and throw them out at the population and hope some of them were read. Now you can swamp your enemy's TV transmitters and reach every household with the message. However, a well-placed bomb or missile could put pay to both of these threats, a bomb on the printing press or a missile attack on the TV transmitter.

[Cohen] Both.

[Dunnigan] Neither.

[Giessler] Both—just as was air warfare and industrial warfare and maneuver warfare and economic warfare and media warfare and...

[Gust] I think technology advances are driving this doctrinal issue. We are now asking what can we do with a technology rather than asking what we want in a technology to accomplish a task.

[Hazlett] Both, some information warfare weapons, such as viruses, trojan horses, etc., are products of technology and therefore technology dependent—and yet—their use is enabled by electronic technology. ISR (intelligence, surveillance and reconnaissance) systems are technologically dependent, but they also enable information attacks by divining and defining an adversary's information posture.

[King] Both. The technology enables systems to be built (very fast computers) but the use of them in information warfare is dependent on other technologies being in place (pervasive networks).

[Libicki] What's the difference?

[Loescher] Technology enabled, I think. There is a pattern in technological revolutions (e.g., oil, automobile, power industries) that begins with invention, moves through systemization and eventually changes the culture. That's what's happening to us now

(probably stage 2). But if you choose to narrowly define the revolution in warfare brought about by the info age as "info warfare" then I have to say we're just doing it more efficiently now than in the past. The issue is not IW, which is evolutionary; but war in the info age, which will be revolutionary.

[Merritt] Both. Many of the capabilities that can be used or exploited today and in the future are and will be dependent on technology. Who would have believed as recently as two years ago that we would have WWW [World-Wide Web] capabilities that could and will revolutionize how we do business. By the same token, it is going to require new technology that currently does not exist to enable us to execute IW both offensive and defensive.

[Probst] I have trouble parsing this question. Clearly, we can't have a Revolution in Military Affairs without unprecedented technology advances. Also clearly, more and more computers are becoming safety critical, or relevant to national security, or whatever.

[Schwartau] Of course it is. That's what makes it possible. For information in war, technology is the enabler, and for Pure IW, technology is the weapon and the target. See above.

[Steele] In the ideal, information war and peace is technology independent, that is to say, a very fine information strategy and information policy, as well as very fine information operations, can be developed and pursued without any enabling technology at all. Right now the offense (the mutts) have the advantage against the defense (the status quo Western powers) because the leverage they can derive from attacking complex technical infrastructures with physical tools (or electrical tools) is enormous. Right now offensive war by anonymous individuals is enabled. Defense is hampered by the complexity of the systems, and the lack of equivalent political and doctrinal arrangements.

2. Commonalities and Differences

Many participants thought that information warfare is both enabled or enhanced by technology and dependent on technology. There are obvious forms of information warfare (such as psychological operations through leaflet drops) that exist outside of modern information technology, although such methods may be enhanced by information technology. Just as clearly, as Mr. Peter Cochrane writes, "technology simply enables new forms of Information Warfare." These new forms of modern information warfare would not exist without technology and are thus dependent on information technology.

Again, there are clear parallels to the development of airpower. Limited early forms of air warfare (e.g., the use of observation balloons in the Civil War) were not dependent on the modern aerospace technologies now in use. But modern forms of air warfare are definitely dependent on such technology.

B. KEY TECHNOLOGIES

Given that technology plays such a key role in information warfare, this question asks about the specific technologies that are currently vital in information warfare. The purpose is to identify and understand current technology as a precursor to discussing future technologies of information warfare.

1. Delphi Responses

[Moderator] What are the current key or enabling technologies of information warfare?

[Campen]
1. High bandwidth transmission.
2. Mass storage.
3. Data search technologies.
4. Simulations.

[Cochrane] Computers and telecommunications technology in all forms seen by "users" (TV, radio, fax, Internet), plus all of the infrastructures that go with them (fixed, mobile, satellite). Mobile computing and communications, including mobile and satellite systems, computing systems of all kinds, well known operating systems and glass, wire and radio networks. (Don't forget the soldier on a motorbike, he is still very useful).

[Cohen] Information technology—as a whole.

[Dunnigan] Hype.

[Giessler] All the wares. Within hardware we can't keep up with COTS [Commercial Off-The-Shelf]—but the chip and the satellite and the EMS [Electro-Mechanical Systems] and the fiberoptics are all intertwined—and we couldn't do anything without mundane things like electricity.

[Gust] Clearly, digital signal processors are the key enabling technologies in our info and info warfare business area. Their increasing capacity and reducing size makes them the choice for the brains in almost any system design.

[Hazlett] Offensive: jamming, global positioning systems, satellites, computers. Defensive: crypto, stealth, computers.

[King] Systems with very large computational and storage capabilities, worldwide high-speed networks, growth in mobile technologies.

[Levien] There is no doubt that the technological base of the Information Warfare revolution is the "Tyranny of the Chip!!" The fact that there has been an exponential growth in the speed and capacity of the semiconductor chip, along with a reciprocal exponential drop in the cost and the size of this same chip, has indeed opened the door to EVERYTHING else that drives information warfare. This is not to detract from the growth in the field of computer design and software skills, but these evaluations were only possible once the semiconductor nerds did their thing. All else derived from the seminal work of Shockley, Bretain and Bardeen at the Bell Telephone Laboratories back in the 50's with the discovery of the transistor.

[Libicki] Other than information systems in general?

[Loescher] The powerful ones haven't been invented yet—but Java is a start at a world of software robots.

[Probst] A partial list includes:
- high-performance computing and communications
- high-performance data assimilation and analysis for centralized intelligence fusion and correlation, and battlespace understanding
- control-theory technologies for automated strategic decision making at the strategic, operational, and tactical levels of war
- major advances in modelling and simulation
- bandwidth negotiation in virtual networks
- information-survivability technologies

[Schwartau] We can go on and on about bandwidth and MIPS [Million Instructions Per Second] and the evolving power of the networks and computers. But I am looking for more than standard old think for IW. I expect to see in the next 10 years:
- Greater mind-man interface
- True VR [Virtual Reality]
- nano-technology weapons (those are fun!)
- Breakthrough cryptanalysis: "There are no more secrets"
- Targetable remote bio weapons (in distinction to mass destruction bio weapons)
- Psychic warfare capabilities should reach the battlefield.

[Steele] Technical access plus hacker-like understanding.

[Todd] The microprocessor and the connectivity between those emerging technologies has defined the information age. The ability to process and distribute information results in great opportunities and challenges for warfare in the information age.[Loescher] The powerful ones haven't been invented yet—but Java is a start at a world of software robots.

[Probst] A partial list includes:
- high-performance computing and communications
- high-performance data assimilation and analysis for centralized intelligence fusion and correlation, and battlespace understanding
- control-theory technologies for automated strategic decision making at the strategic, operational, and tactical levels of war
- major advances in modelling and simulation
- bandwidth negotiation in virtual networks
- information-survivability technologies

[Schwartau] We can go on and on about bandwidth and MIPS and the evolving power of the networks and computers. But I am looking for more than standard old think for IW. I expect to see in the next 10 years:
- Greater mind-man interface
- True VR [Virtual Reality]
- nano-technology weapons (those are fun!)
- Breakthrough cryptanalysis: "There are no more secrets"
- Targetable remote bio weapons (in distinction to mass destruction bio weapons)
- Psychic warfare capabilities should reach the battlefield.

[Steele] Technical access plus hacker-like understanding.

[Todd] The micro processor and the connectivity between those emerging technologies has defined the information age. The ability to process and distribute information results in great opportunities and challenges for warfare in the information age.

2. Commonalities and Differences

Broadly construed, the answer as to what are key information warfare technologies is "all information technologies." More specifically, the important technologies identified could be boiled down into a few general areas:

- Mobile and fixed high bandwidth transmission capabilities via various means
- Modelling and simulation advances
- Computers with massive processing capabilities
- Increased mass storage
- Data search, analysis and fusion tools
- Ubiquitous and cheap CPUs and digital signal processors
- Sophisticated cryptology
- Standard and widely-used operating systems (like UNIX)
- Electricity[1]

Finally, one point made by Dr. Fred Levien bears further emphasis. While all the various information technologies play important roles in information warfare, much of this progress is dependent on the continued growth in the power and speed of microprocessors along with the accompanying drop in cost and size. This relationship has held true throughout the development of the microprocessor, but will it hold true in the future?

[1]As Dr. Fred Giessler points out, underlying most of these technologies is the requirement for electricity. This category of technology could be labelled more generically as "power sources and batteries."

C. THE BEST OFFENSE IS A GOOD DEFENSE?

Information warfare is generally thought to have both offensive and defensive components (Defense Science Board, 1994). Obviously the strategies and techniques for these components are different. But is the same true of the technologies to support offensive and defensive information warfare? This question examines whether there are distinctions between the two technology sets.

1. Delphi Responses

[Moderator] Are there differences between "offensive" and "defensive" information warfare technologies?

[Campen] Depends. An offensive technology is constructed to exploit a known vulnerability in a defensive technology. Example: A virus and a firewall both use software technology. A defense against an electromagnetic attack might be a fuse, a shield or physical separation.

[Cebrowski] Information itself is the basis. Information technology is the broker, tool and application, in different ways. As such, technology serves to shape and present information. The control over how, how fast and how accurately information technology works on and with information is the essence of both offensive and defensive information warfare.

[Cochrane] The underlying technologies will be the same in both situations—it is just a matter of how they are used and where you sit as to whether they are offensive or defensive. E.g., if you write a software agent that goes around all the systems it can and gathers information then from your point of view it is a defence agent that spots enemies. To the person owning the system it is an offensive piece of technology. Offensive strategies are likely to require highly trained teams with specialised knowledge. Defensive technologies will include information monitoring and filtering together with computer and network resilience and healing techniques. Some have said offence is easier than defence but that may not be the case. A direct attack might be easy to mount but could be easier to trace back to the originator.

[Cohen] Yes. To be a good defender, you have to understand all about offense and find cost effective ways to provide adequate protection against the wide range of offensive potentials. To be a good offender, you have to find a hole and exploit it to your ends. The technologies for doing this are quite different.

[Dunnigan] Not really.

[Giessler] Many if not most overlap. Generally they are two sides of the info technologies coin. And you must consider both sides as you contemplate the coin. And you must consider the coin with two sides and a center as a system—that is fully connected.

[Gust] The Army labs here at Monmouth always give a sample of new info technology, i.e., a new radio, to the IEW [Intelligence and Electronic Warfare] Directorate to see if it has certain vulnerabilities or can be defeated easily.

[Hazlett] Yes, some systems, such as crypto are inherently better suited for defense; while others such as active electronic or acoustic jamming are offensive.

[King] Yes. Internet security gateways are defensive weapons. There are some systems that attempt to detect threats and then try to go on the offensive and track them down. Defense is harder as it has to cope with a great variety of different offensive systems.

[Levien] The difference between "offensive" and "defensive" IW technologies are to my mind almost all legal ones. There is of course the differences in perception that has been recently highlighted between the Army and the Air Force as how to wage the new IW warfare. The really tough question is how to ask a military officer to "defend his country against all its' enemies whomsoever...foreign or domestic" when you cannot clearly tell him who his enemy really is, and then threaten him with courts martial if he makes the wrong choice in the small instant of time he has available before he must act given the great body of legal garbage that awaits (much of it contradictory) for the Monday morning quarterbacks to quote from after the fact.

[Libicki] What differences exist are relatively minor (techniques of infoint collection are probably offensive in nature while CCD [Charge Coupled Devices] technologies tend to be defensive), and hard to distinguish.

[Loescher] Yes, technologically. However, operationally, the dual necessity of offensive and defensive actions is vital. In Navy, C4I is becoming more and more splintered, lacking advocacy, while IW, which in Navy is cryptology reinventing itself, is prevailing. That's a mistake. For the U.S., information is primarily a force subtractor at this stage because our dependency on it holds us tactically, if not strategically, banking on it. If you ask yourself what a small country can do to defend against an overwhelming military force, the options are clear. We need C4I more than we need offensive IW—though both are important. Unfortunately, in Navy, they are dividing. I see my job as helping to restore that balance. However, the technology of IW is tangible, while the promise of C4I is still in viewgraphs. That's a hard—but vital—sell.

[Merritt] You bet. Defensive will be a lot harder, on all fronts. A lot of work remaining to be done. How do you do reconnaissance? What sensors do you need? How do you do IW Indications and Warning? How do you build countermeasures that don't become obsolete immediately?

[Probst] If we use these words they way I have defined them, then they are quite hard to separate. I would imagine that anyone skilled in one would be reasonably skilled in the other.

Sometimes it helps to solve a simpler problem first.

Computer-aided Postal Chess

White and Black both have chess computers that function as "brain multipliers". The chess computers have a chess rating, and can be set for different levels of play.

The leaders of the Revolution in Computer-Aided Postal Chess have ordered you to trade in your expert computer for a grandmaster computer.

Offense and defense change in subtle fashions:
- if I upgrade my chess computer, that does not ipso facto downgrade your computer, but it does give me an advantage
- if I break into your house and monkey with your chess computer so that it surreptitiously plays at less than full strength, that's a "Level-3 IW attack" :-)
- if I change the locks at my house, so that you won't be able to reply in kind, that's "defensive information warfare"
- if you cut off the supply of electricity to my house, you have attacked my infrastructure
- and so on

[Schwartau] In order to defend, you have to know the offensive capabilities, so there is a great deal of similarity, although the techniques are different. I would have to write out a chart, but it would include thoughts like:
Sniffing Crypto
Sniffing Authentication
Viruses Smart O/S
Laser Interception Masking
PsyOps Truth Police
and so on. Good question with an infinity of possible answers.

[Steele] Offense is much much easier and can be physical as well as electronic. Defense is an order of magnitude more complex and expensive.

[Todd] Based on the comments to this question, there appeared to be a predominant notion that offensive and defensive technologies referred to hardware aspect only. While technologies are themselves "hardware," I think a point might have been lost. During the Korean War, the MIG-17 was superior in hardware (performance) to that of the earlier model F-86s. However, the American's retained a superior combat record of 10:1 over the adversaries. In this case, your superiority in training and combat tactics mitigated a technological inferiority. So it is in IW. Our risk analysis indicates that the better training and education of the user and systems administrators results in a far superior investment vs. results scenario that merely "engineering in" defensive solutions.

2. Commonalities and Differences

To a large extent, the group felt that the underlying technologies for performing offensive and defensive information warfare are the same. While there may be technologies

that are more suited to one or the other, in general the difference is more in how the technologies are used (the application or technique[2]) than in any underlying difference in the basic technologies. Several group members also thought that information warfare defense is much harder than offense because the defender must understand the techniques and technologies of all possible offensive attacks, while the attacker need find only a single vulnerability in the target information function.

D. INFORMATION WARFARE SYSTEMS

Much of the acquisition process is built around the development and fielding of systems. As a lead-in to future discussions about information warfare acquisition, this issue asks about what might be regarded as an "information warfare system."

1. Delphi Responses

[Moderator] What can be considered an "information warfare system?"

[Campen] The assemblage of people, processes, equipment and software needed to wage conflict in the electromagnetic spectrum and protect itself against attack.

[Cebrowski] There is no "pure" information warfare system from a technical or weapons system standpoint. Weapons systems can perform information warfare functions, but as a byproduct of technical design. However, an information warfare system can be defined in terms of a series of interrelated processes that include technology. For example, an information warfare process may consist of established standards and scope for information protection, coupled with adequate attack detection and restoral tools and techniques.

[Cochrane] An information warfare system is any collection of resources that can be utilised in order to further your aims in a conflict by disseminating or disrupting information. E.g., lorry packed with a fertiliser bomb can be a useful information warfare

[2]Col. David Todd makes the point that throughout the history of war, good techniques and proper training have often compensated for inferior technology.

system when driven into the country's central bank. The most critical element of ALL information warfare systems is the human brain. It will always find a new way of adapting an innocent system into something that can be used for a more devious purpose.

[Cohen] All systems are IW systems in some sense. It's their USE and not their CONTENT that dictates their involvement in IW.

[Dunnigan] General U. S. Grant standing next to a telegraph operator...

[Garigue] A group of knowledgeable individuals and a truly modern on line library.

[Giessler] Any set of elements related to one another with a goal of survival in the information age. Such a system has input, process, output and feedback. It is a complex-adaptive system that is teleological—goal oriented. So—a commander and his trusted agents (sometimes known as staff) who is trying to defeat, deter, influence the competitor is a I.W.S. So is a HARM [High-speed Anti-Radiation Missile] launched from any kind of vehicle. So is a kid with a virus attacking your info system with the objective of killing it. I.W. Systems are everywhere.

[Gust] An info warfare system is probably best defined by the financial programmatic weapons platform it rides on—JSTARS, Rivet Joint, Guardrail, etc. That would include comm links, ground stations and control nodes.

[Hazlett] Example of an information warfare system: an "active computer firewall/gateway" that detects attempted intrusions and attacks (and conducts counterattacks), yet still permits access by appropriately recognized systems. Example of an information warfare "system of systems:" An active ISR-RSTA [Intelligence, Surveillance, Reconnaissance-Reconnaissance Strike Targeting Architecture] combination that detects attacks on component systems and directs defenses and counterattacks.

[King] A collection of people and systems used to perform an offensive or defensive operation in an information war.

[Levien] Other than a speeding 30-06 bullet, or a hand grenade...about all remaining military systems fall into the IW system category.

[Libicki] An A-10 with a GAU-30 [Note: this is a 30 mm cannon] will work just fine if there is a command center or puter system underneath.

[Loescher] Let me answer it this way—the best system for IW is the operator's mind. The rest is trapping.

[Merritt] I addressed some of this earlier. A lot of possibilities. Many of which already exist, but haven't been deployed in a coordinated manner that would have impact on perception management on the battlefield. It is much more than a network issue.

[Probst] Above all things, an integrated battlespace management system that uses data-intensive predictive modelling and simulation.

[Schwartau] Me. You. A hacker. The bad guys. The system comprises the technology + motivation. Technology by itself is neutral; not bad or good. Remember, for example,

that the only difference between a programming error and malicious software is intent. Or, that at a microwave repeater if properly tuned and aimed creates a fine DOS [Denial of Service] device.

[Steele] Any form of strategic thought, policy, or organization, which may or may not include technology, that seeks to achieve a specific information objective.

[Todd] An information system consists of a system of sensors (either organic or electro-mechanical/electromagnetic), the linkage to human decisionmaker or assessment center, the linkage between that decisionmaker (electromagnetic, mechanical, etc.) to a combat system, and the sensory feedback. I very much agree along the lines of links, nodes and human elements comprise a IW system.

2. Commonalities and Differences

Several thoughts emerge from the above comments. The first is that an information warfare system is more a combination of elements working together to perform information warfare functions than a single identifiable end-item. These elements could include hardware, software, policies, procedures, and perhaps most importantly, human brains. Thus Admiral Cebrowski's remark that there are no "pure" information warfare systems in the sense of the traditional weapons systems or platforms.

The other common thread once again deals with the issue of means versus ends. From this standpoint, any system can be an information warfare system depending on how they are used. Employing a hard kill or a "kinetic solution" to take out a target qualifies the particular attacking system as an information warfare system when used against an information function such as a computer system.

E. SYNTHESIS

The relationship between information warfare and information technology is deep and fundamental. While many methods of information warfare can exist independent of

technology, their effectiveness and military usefulness can be greatly enhanced by information technologies. There are also a number of modern methods that are completely dependent on information technologies. In general, these technologies are the same for both waging offensive information war and for protecting against information attacks—only the techniques and applications are different. This implies a need for close ties between those developing and using technologies for offensive purposes and those developing and using technologies for defensive purposes.

In terms of specific technologies, the participants identified a number of presently important information technology areas. There were also technologies not mentioned, but which seem key for information warfare. These include the development of tools and methodologies to support the design of very complex industrial-strength software and the advances in miniaturization which allow the incorporation of generic information technologies into smaller and smaller end-items. And while not necessarily a "technology," the establishment of common standards for interoperability and data exchange are a prerequisite for the enhanced connectivity so important in the information age. Including these yields the following categories of vital technologies:

- Technologies that allow connectivity
- Data storage, fusing, and extraction tools and technologies
- Modelling and simulation techniques
- Technologies that allow for security through encryption
- Tools and methodologies for development of complex software
- Miniaturization techniques
- Power and battery technologies
- Common standards for interoperability and data exchange

Finally, with a few exceptions such as electronic warfare platforms, there do not seem to be cleanly segregable information warfare systems in the traditional sense. Dr. Andrew Marshall, the DoD Director of Net Assessment, recognizes this when he states, "these technologies do not seem to promise some distinctive new platform around which a revised doctrine and force structure can be built" (Marshall, 1994). Much as C4I systems, information warfare systems are more collections of hardware, software, procedures and people. This has development and acquisition implications that will be explored shortly.

IV. IMPLICATIONS OF COMMERCIAL DEPENDENCE

> Information system superiority is dependent on an ability to incorporate the latest in commercial technologies.
>
> — Defense Science Board Summer Study, 1994

Driven by tight budgets and a need for cost savings, dependence on all manner of "off the shelf" commercial technology, products, and standards is fast becoming a way of life for the military. Use of commercial technology is promoted at the highest levels and this is especially true for information technology. This topic is concerned about some of the broader information warfare implications of such increased dependence on the commercial sector.

A. THE INFORMATION WARFARE EDGE

One hallmark of commercial technology—with some few exceptions—is that many commercial items are available for purchase to anyone who has the money to buy them. This is especially true in the case of commercial information technology, where some items are produced by potential enemies and most items are procurable by potential enemies (Christian, et al, 1995). Thus possible foes will be able to obtain the same basic information warfare technologies in use by the United States or its allies. If the above is true, then sole access to the latest technologies will not be guaranteed. In this

technologically-levelled playing field, what will give one side or the other an advantage in waging information warfare?

1. Delphi Responses

[Moderator] If everyone (including potential adversaries) has access to commercial information technologies useful in information warfare, then what will give the U.S. and allies an edge?

[Campen] It is not a question of access, it is a question of the timely and innovative exploitation of that technology.

[Cebrowski] The edge comes in the synergistic application of technology. For DoD, it's organizing all the IW elements as a system, then integrating it into the larger system of warfighting...in a way that enhances ops tempo. Technology is only an enabler. The real power comes from organization and employment concepts. If we don't tackle this area soon, we will lose the lead!

[Cochrane] Access to commercial Information Technology does not of itself define an edge in Information Warfare. Advantage in warfare is not just the possession of weaponry, it is its effective use and the knowledge of how to survive in order to use it again in a combat situation. This edge can be gained during the development, trailing and training in Information Warfare techniques. The scale of investment and technological inertia in the commercial sector will only slightly reduce the scale of the advantage that military strategists would like to attain.

[Cohen] The non-COTS [Commercial Off-The-Shelf] part—the way we connect things together—the way we use things—the skill and training and education of the people using them. We may, in fact, not have an edge.

[Dunnigan] Yes. We have more experience and resources in NetLand and, all things being equal, should prevail (Napoleon: "Victory goes to the bigger battalions." Unless they're Austrian, of course...)

[Garigue] The differential comes from the software. Let's not forget that it is the software that make the machine. There can be some substantial capability gains that come from the usage of COTS in Life Cycle Management areas such as costs, availability, acquisition, disposal etc.. but the real warfighting advantage will come from the "configuration" of these software machines and the resulting networks that are developed to support enlightened decision making. Multiplied by the net, one software program can be replicated in each machine and because of this flexibility thousands of more knowledgeable decisions can be made. The network can now distribute knowledge very rapidly. So it is the software (and the wetware) that confers new information warfare capabilities to the organization, COTS is simply the delivery method.

[Gust] Not everyone has access to all commercial info technologies. In addition, my PEO [Program Executive Officer] has recently had a requested FMS [Foreign Military Sales] sale of Night Vision goggles to an ally be disapproved by HQ, DA [Headquarters, Department of the Army]. There still has to be some area of exclusiveness for the U.S. forces to retain a technological edge.

[Hazlett] Innovative organizational concepts, accelerated and automated decisionmaking, and more flexible and automated communications routing.

[King] The edge will belong to those who develop a strategic plan and are willing to make the investments necessary to always be ahead of the wave and not merely on it. The U.S. currently has an advantage in its knowledge and deployment of high-speed nets.

[Probst] Two short answers:

- articulate the new operational concepts so that we can have a Revolution in Military Affairs
- exploit the U.S. edge in superior doctrine, superior machines, superior algorithms, and deployed effective Defensive Warfare

[Schwartau] We have to do a couple of things:

1. Make sure that the military still has an edge up on technology that does not reach the commercial sector. This is true with the nature of the DEW [Directed Energy Weapons] (HERF [High Energy Radio Frequency] style weapons) that the military develops. They are vastly more powerful and useful than the homebrew commercial versions. We must take similar approaches with related "weapons."

2. We have to build an organization that is capable of C4I style deployment and engagement to either avoid conventional conflict, or replace conventional conflict.

[Steele] The U.S. and allies can only have an "edge" if they stop lying to themselves and admit that the existing communications and computing industries are "out of control" and ignorant if not criminally negligent with respect to C4I security. The "missing link" in IW is a secure home front, and this requires a national program—understood by and supported by the people—to embed decent security in all U.S.A. produced cyber-products. This will, incidentally, give a boost, to U.S.A.-based producers, whose security "quality" will serve as a major market differentiator. Included in this new commitment to security (and all it implies in terms of data integrity, etc.) will be the ability to detect and eradicate foreign-produced viruses and backdoors—for instance, the industry today is compounding its traditional failure to document software code with the outsourcing of much major code production to Calcutta and Moscow. We have <u>no idea</u> what these people are putting "between the lines" and we should be very concerned.

[Todd] Do not necessarily agree that all potential adversaries will have access to commercial information technology...certainly the possibility is there, but to what degree. Likewise, while other countries may "leap frog" us in more state of the art technologies (go from no telephone service to cellular phone service and bypassing telephone wires), the market place may dictate how and what is available. This disconnect between 2nd, 3rd, 4th generation telecommunication systems, networks, and processing capabilities will enable us to analyze the "seam" in their architecture and exploit them.

2. Commonalities and Differences

The first reaction to this question, as pointed out by several participants, is that there will always be some advanced and unique technology only available to the military. Thus these unique technologies will be one part of any information warfare edge. Another possible area for gaining an advantage is how well a country or organization is able to develop and implement the doctrinal and operational concepts required to take advantage of information warfare. Related to this area is how well an organization adapts its structure to develop information warfare capabilities, especially in terms of developing people with the right skills, training and education to effectively conduct information warfare activities.

Finally, there were two more technologically oriented answers. The first is that simply having the technology is not enough. How effectively and how fast such technology is integrated and exploited is the real key to any information warfare edge. The best technology improperly integrated and/or exploited in a tardy manner will be of little use when faced with slightly less advanced technology correctly integrated and available now. Lastly, LCDR Robert Garigue argues that software is the key "differential." Hardware items are typically general-purpose tools and it is the software that embodies the "brains" of most information systems. How effectively one is able to configure and lash together systems via the development of good software could provide the crucial information warfare advantage.

B. INFORMATION TECHNOLOGY INTEGRITY

Within the government and military, there is an ever-increasing reliance on hardware and software developed completely outside of government or military channels.

With this reliance comes a concern for the integrity and general security of products obtained on both the domestic and global commercial markets. In additional to domestic software and information technology development, software coding is being outsourced to places such as Russia and India and integrated circuits are being developed in countries all around the world. During such development, there are opportunities for the insertion of malicious software code or circuit paths into normal commercial products that may eventually be used in government or military information systems. How these possibilities might be addressed is the next topic for the group participants.

1. Delphi Responses

[Moderator] Given the possibilities for "chipping" and software "backdoors," how do we ensure the integrity of domestic commercial manufacturing and software processes? How do we ensure the integrity of foreign commercial components and systems which we might use?

[Campen] You don't even try. We must presume this threat and concentrate on the means of extremely rapid detection, fault isolation, and corrective actions.

[Cebrowski] Demonstrate to naysayers that the issues can be managed within reasonable cost. The key is to establish a systemic, national-level process that includes: scope and standards for what should be protected and to what extent (a risk management process); responsive indications and warning/attack analysis; and a broad range of flexible response options. This process will not demonstrate a nation that is invulnerable, but rather one which is constantly vigilant, decisive and prepared to respond to any threat, foreign or domestic, with a full range of national security tools.

[Cochrane] Chipping and "backdoors" are as much a problem to commercial entities as they are to the military. An attack on a large banking institution may cause as much damage to a nation as an attack on a military installation. Existing examination of systems based on guides such as the Orange Book are of limited use. Experience has shown that these processes are difficult to "sell" to software developers. To complement this we need to develop penetrative testing in ways that simulate real attacks and study how systems will react.

[Cohen] With rare exceptions, we don't, and that's an important issue today.

[Dunnigan] You can never let up your guard on such things. Put it out of sight and you can expect the bad guys to come in through your back door.

[Garigue] There will never be any guarantee that software will be proven correct and have no "defects" because of the enormous difficulty of checking large complex programs. Networks are even more problematic. The analysis can only be limited to small portions of programs or objects. And even when programs can be proven correct, there still would exist the possibility for perfectly correct code becoming malicious (Jekyll and Hyde programs). Partitioning mission critical processes from other processes, and ensuring that some functions be performed via an agency of differently coded processes does enables a certain measure of redundancy, cross checking of results, and graceful degradation of performance.

[Gust] This is an area where integrity of use requires adherence to patent and license concerns. We should pay for software intellectual rights if we use it in our systems.

[Hazlett] Developing and instituting a "red team" concept for testing and evaluating software. Developing an "overlay" for domestic and foreign software and components, that detects and reports intrusions and alterations.

[King] There are processes and methods that can be put in place but there will always be the question of the cost of achieving a given level of assurance and the impossibility of that level being 100%. Thus, systems must detect and contain suspicious subsystems (not an easy problem).

[Probst]
- legal requirements for due diligence with severe financial penalties
- never trusting software you haven't (re)written yourself
- spreading the "public health" approach to component integrity
- eternal vigilance following adequate training (e.g., personal monitoring of personal audit trails—cf. Shimomura)
- less practical: never trusting hardware you haven't designed yourself (testing and certification may be of some help here)

[Schwartau] Someone read my book! Thanks. That's the problem. We will have to develop new methods of process engineering, assurance mechanisms and automated reliance tools. Similarly, we will have to develop additional non-destructive testing methods for completed products as an inspection or QA [Quality Assurance] procedure.

[Steele] The Department of Commerce is simply not up to the challenges of the 21st Century (neither is much of the rest of the USG [U.S. Government], but at least DoD knows there <u>is</u> a 21st Century). The first step must be legislation which requires "due diligence" on the part of all manufacturers and vendors of communications and computational hardware, software, and related services. They must be <u>required</u> to assure their customers that it is safe to work and play in cyberspace, and must be held accountable, using new and solid international standards, to the highest levels of embedded security. The U.S. position on key escrow is ignorant and flies in the face of both history and cyber-power. Until we give up the idea of legislating back doors for law enforcement, we will not be able to provide common security to the whole.

The FBI should be given funding ($500 million a year) for a new Electronic Security & Counterintelligence Division, and the Secret Service should be relieved of its dubious claims to the mission of handling crimes in cyberspace. National testing & certification laboratories should be established using <u>existing</u> capabilities (for instance, one of the

Department of Energy laboratories), and all foreign hardware and software should be subjected to both preliminary and ongoing (random) testing. All hardware and software being introduced to government installations should be individually tested. Corporations should have liability incentives for doing the same thing. Ultimately we should eliminate portable disks and require that all data and software be sent from one infosec gate to another for scanning and air gap transfer under control.

[Todd] The ability to protect our systems needs to be the first priority in this emerging warfare area. Our first goal is to raise the our integrity of our systems to such a level that the "casual" hacker cannot get primary access to our network system. This can be done with an integrated approach of engineering fixes, highly trained system administrators, and highly aware users. This will have to be a continuing effort. But we will still need to understand that the top 5 percentile of professional hackers will still be able to penetrate our system. Now we need a system of both highly trained people and equipment that can identify such activity, bound its effect, recover systems that are damaged or corrupted, and work back to the origin of the attack for either criminal prosecution or counterintelligence activities.

2. Commonalities and Differences

The group took two basic approaches[1] to this question. The first approach lies with what the manufacturers and commercial firms must do themselves in order to assure product integrity. It is suggested that firms construct much better ways to check and ensure product integrity through new methods of engineering, assurance checking and developmental testing. Then once a vendor has sold a product, it is certifying both a given level of security assurance to the customer and that it has exercised "due diligence" in the development of its product. The term "due diligence" implies a legal duty to a customer, a breach of which is punishable under law. This provides a financial incentive for firms to seek product integrity.

[1]The Defense Advanced Research Projects Agency (DARPA) has taken a strong interest in both of these areas. It is currently funding dozens of efforts in the fields of high confidence networking, high confidence computing systems, development and integration assurance, and survivability/vulnerability techniques and tools (DARPA, 1996).

The other approach to this problem deals with what the customer should do to protect themselves from products of unknown integrity. Under this view, it is not possible or wise to assume the integrity of any product and a certain amount of vulnerability is presumed. Then activities are taken to mitigate any hazards. Such activities include risk assessments, development of means for threat detection, and implementation of a scalable range of comprehensive assurance testing for commercial hardware and software. In addition, larger systems can be designed to combat malicious code or chips through architectures that support redundancy and partitioning of critical elements.

C. INFLUENCING COMMERCIAL DEVELOPMENT

The previous question highlighted the fact that commercial firms may be able to address many of the military's information protection concerns during the product development cycle. But with a declining overall DoD budget and a rapidly growing commercial sector, DoD's share of the commercial information technology market is growing smaller and the military has less market influence than it once had (Berkowitz, 1995). With such declining influence, how should the military incentivize vendors to take (perhaps) unique security requirements into account in the building of commercial products later purchased off-the-shelf by the military.

1. Delphi Responses

[Moderator] Given the decreasing financial leverage of the military in the commercial marketplace, how should the military positively engage firms to take military needs into account during the commercial product development process?

[Campen] First you take into account the remarkable similarities in "needs" between the private and military sector and identify short falls. The military then applies its talents and funds on those relatively few shortfalls.

[Cebrowski] This is achieved by answering and addressing two questions: What must be protected? Certainly not "everything." This is the policy issue on the scope of protection. What type and level of protection is appropriate, under a managed risk approach? This is the technical question of "standards." Those commercial organizations wishing to "do business" with the protected enclave must interoperate on its terms. Over time, the standards become universal—not by mandate, but by market forces.

[Cochrane] By locking companies into the development cycle as the military outsources everything. The military is still doing studies, still funding universities, still doing original stuff. Forming a partnership with companies on joint programmes where there is a synergy between the applications. What is the difference between secure banking, secure networking for industry, and the military—only degree!

[Cohen] Money.

[Dunnigan] Pay them money. That always works. Beyond that, the troops have little influence.

[Garigue] I believe that that is not required. The present capability of components and systems by far exceeds the present majority of our needs. The notions that competitive advantages will come from faster, smaller, more secure, robust, and functional information systems are already accepted goals and are driving every commercial innovation process. We need not emphasize these expectancies. However, we do need a more focused effort on the problem of how to use these capabilities to impose order or defuse conflict.

[Gust] We use a dialog process in the Army which includes Advance Planning Briefings to industry and discussions via an electronic bulletin board for draft RFPs [Request for Proposals]. We also speak to symposiums and industry forums. Finally, pre-solicitation conferences advertise the near-term release of the RFP to the interested bidders who responded to our CBD [Commerce Business Daily] announcement.

[Hazlett] Revise acquisition procedures so that government specs do not needlessly burden process. Revise "lowest bidder" rules so that government can purchase "best value."

[King] The military needs to be very clear and realistic about how its needs differ from commercial needs. There will continue to be companies that make mil spec versions of commercial products for those few cases where they are really needed.

[Probst] Build military applications on top of COTS hardware and software. If you really need something different, talk to them.

[Schwartau] Declassify the threat to the commercial sector. Put us all on the same team.

[Steele] Declassify the threat. Not only will the private sector not heal itself until it fully appreciates the problem (and stockholders know enough to hold management liable for being stupid about electronic security), but the military will never heal itself as long as C4I "deficiencies" are classified—the latter guarantees that only the people that created the problems in the first place will have the clearances to jerk around with possible solutions, oblivious as they are to the explosion of innovation in the private sector, far from all SCIFs [Sensitive Compartmented Information Facilities].

2. Commonalities and Differences

One of the commonly voiced thoughts on this question is that there is a remarkable correlation between the information protection needs of the military and the needs of those in the commercial world who seek secure banking, purchasing, networking and databases. The overlap is great and there are few unique military requirements. For those singular areas, the military should clearly identify its needs and "pay money" for the commercial vendors to include the features directly or add the hooks necessary for the military to add hardware or software on top of the commercial item.

Finally, the point was made by several participants that the best way to ensure that commercial items include some measure of information protection is to "declassify the threat." Sharing (in some manner) the information warfare threats and vulnerabilities already identified by the government would allow commercial establishments to apply their own resources against these vulnerabilities. Fixes made and included in their products going to market will then benefit the military when it buys such products.

D. LEARNING FROM COMMERCIAL FIRMS

On one hand, the military might have useful information protection data it could share with commercial firms. Likewise, non-military enterprises that use commercial information technology also may have something to teach the military in this area. This question addresses what and how military and commercial activities can learn from each other.

1. Delphi Responses

[Moderator] Many commercial firms (for example, banking firms) share the same "information protection" concerns as the government. What can the military learn from how these companies conduct information warfare functions? How should we share this information?

[Cebrowski] This first step is to raise awareness of senior level management and encourage dialog in interagency fora. An understanding of the inherent vulnerabilities of information-based technologies will spawn focused efforts on security processes, procedures, and policy. If we can learn anything from the commercial sector, it's the extremely low tolerance for ignoring security policy. Before this can be done at the scale and levels required, government must put in place the policies and legal protections necessary to secure interests and equities.

[Cochrane] Such commercial enterprises have communications and systems that are often held by, or accessible by, "the enemy" and are open to attack on more than one front. Commerce probably has simulated and experienced a greater number of attack scenarios and now can respond to an attack faster than the military. Information technology is the life blood of a modern nation, if it is cut off then society crashes and stops. Sharing is only a problem for the military; they will just have to get used to the idea!

[Cohen] These firms do a poor job of it in military terms, but the military could, at a minimum, adopt the same minimum standards these firms use in addition to current DoD standards.

[Dunnigan] You mean, "how do you get them to share information with you." The banks are in real info-war mode at all times. These are the folks with the "combat experience" regarding what works and what does not. In the peace time, the military is playing games while the banks are battling the hordes of cybernasties.

[Garigue] Open societies as well as open systems are more robust because the spread of critical information and knowledge on security helps everyone. Continuing an open dialogue at all levels between the concerned groups such as between the banking, power, telecom, and military communities as well as with the security advocate groups within

Internet will ensure that the weakest network functions will be identified and brought into line with acceptable security procedures. What benefits one community, benefits the net and benefits all communities.

[Gust] There is a formed chartered organization in the Army, supervised by the HQ, DA DISC4 [Director of Information Systems and C4] office responsible for the "C2 Protect" mission. I am not totally current on the details of their involvement with commercial businesses, but know that a process is in place.

[Hazlett] Government should fund a portion of the research so that it can benefit from the discoveries and be part owner in the product. Share in licensing the procedures and products.

[King] There is a lot to be learned but it will be a difficult process. There are signs such as the "Invitational Workshop on Computer Vulnerability Data Sharing" scheduled for June in Gaithersburg that this is recognized as a common problem that must be solved.

[Probst]

- Banks worry about information security and banking-systems security. Certainly one should talk to their security officers. I really doubt that banks crack other banks, so you won't find much help here.

- The ISAT [Information Science and Technology] Summer Study on Defensive Warfare and Information Survivability had a balanced mix of academic, commercial, and government representation.

- As the market develops, people will buy the security products they need (the government's role is primarily to watch over the infrastructure).

[Schwartau] The key lesson is that much of the commercial sector can move on a dime; unlike slowing down a carrier in 20 miles.

- Rapid Decision making
- Iterative process changes
- Adaption to market conditions
- Policy must change as rapidly as do one's adversaries

[Steele] Most commercial firms do not understand electronic vulnerabilities, in part because most of their security and "infosec" officers don't really understand the insides of their systems, and in part because corporate management will continue to shoot the messenger until such time as they cross a major pain threshold, i.e., are held accountable or "see" the losses they are incurring. The real hard problem with electronic theft, as Toffler and others have noted, is that electronic property can be in two places at once—when proprietary information is stolen, the files are still "there," they have simply been duplicated.

Banking has nothing to teach us, despite the inflated claims of some self-serving commentators. The real experts (e.g., Eric Hughes of Cypherpunks) know how easy it is to penetrate both banks and trading houses, not only electronically but also through direct access to uncontrolled terminals on the trading floor. More simple denial of service

attacks, and physical interruption of services, have long been described by Winn Schwartau. The single greatest danger to much of the U.S.A. is the chaos and anarchy as well as the financial loss that will be incurred because of the lack of hard-copy backup documentation for electronic wealth and property ownership. It will take years to sort it all out, and will probably require some emergency legislation freezing all claims.

2. Commonalities and Differences

For the most part, participants thought there was valuable information to be learned from business firms. While to a certain extent the operating environment and the nature of the threat which commercial firms face may be different from the military, many of the systems in use by the commercial sector are the same as ones used by the military. In particular, banking, utility, telecommunications, software and computer companies, along with various security groups, share many of the same challenges as the military.

As to the mechanism for distributing information between these parties, some interaction is already occurring in an informal or ad hoc fashion through studies and workshops. Admiral Cebrowski sees the need for establishment of more permanent and formal "interagency fora" to address this issue. But as a precursor to forming of such groups, there must be government action to construct the policies and legal framework needed to assure industry that shared information of a proprietary or sensitive nature will be protected. Finally, overcoming industry's fears of sharing their private data is very much similar to overcoming the military's fears about sharing "classified" or sensitive data with others. Cultural changes may need to occur among both groups before useful dialogue can take place.

E. SYNTHESIS

It is evident that military dependence on commercial information technology is profound and irreversible. Such technologies will also be largely available to all comers, reducing any purely technological edge to those few items that the military is able to develop itself and/or keep closely held. So to gain an overall information warfare advantage, progress is required in two general areas. First, one must make the structural, organizational, doctrinal and educational changes[2] necessary to develop and wage information war. Second, one must cultivate the timely and correct integration, exploitation and synergistic application of commercial and military-unique information technologies, especially through the use of adaptable and reliable software. The Defense Science Board nicely summed up this perspective in their 1994 Summer Study on battlefield information architecture when they wrote:

> It will be important to stay abreast of current and emerging technology but our real discriminator will be our ability to continuously infuse these technologies and to configure and reconfigure the ensuing products to support joint warfare. (Defense Science Board, 1994)

Fortunately, America's open society gives it what Dr. Joe Nye and Admiral (Ret.) William Owens call an "unparalleled ability to integrate complex information systems" (Nye & Owens, 1996).

In addition, it is clear that the dependence of the military on the commercial world and the intersection of interests between the military and commercial sectors is large enough to make pursuit of cooperation an important task. Issues of product integrity, upfront consideration of security concerns during product development and the potential benefits of

[2]These changes track closely to the last two steps of a generic "revolution in military affairs" as mentioned in Chapter I.

information sharing are all ripe areas for collaboration. Despite the declining military market share, it is still a major player in terms of raw dollars. While the military is certainly not big enough to buck major market trends, it is big enough to exert some influence. This is especially true in areas where military concerns coincide with the concerns of the overall market so that teaming with industry would be beneficial to all.

Mechanisms to promote such commercial-military teamwork already exist in other areas. For example, the Civil Reserve Air Fleet program involves the upfront infusion of military dollars to make certain modifications (like adding strengthened floors and larger cargo doors) to commercial aircraft which make them more militarily useful. In return, these aircraft can then be used during times of crisis (such as Desert Shield/Desert Storm) in support of military needs. This approach could be adapted to support information warfare by engaging in a similar "modification" of commercial information technologies. Military funds could be used during the development of purely commercial information technology wares to promote the insertion of specific security features or the inclusion of built-in "hooks" for the addition of military unique add-on security technology. Likewise, the military could lend some financial support to the development and implementation of methodologies designed to promote product integrity of commercial items.

Another model for commercial-government engagement is the National Security Telecommunications Advisory Council (NSTAC). The NSTAC advises the President and Executive branch on telecommunications national security and emergency preparedness issues (NSTAC Fact Sheet, 1996). True to its name, the NSTAC is focused on telecommunications and its members are drawn primarily from the ranks of communications company chief executive officers. But the NSTAC approach could be

adopted by either expanding the NSTAC or by forming a similar body to consider issues over the broad range of information technology—to include telecommunications, software, computer systems, networks, etc.

While any NSTAC-like body would be considering issues at a high policy level, there would also be a need for a mechanism to promote engagement at the lower levels on day-to-day information protection issues. One such organization already in existence is the government-funded Computer Emergency Response Team (CERT) run out of the Software Engineering Institute at Carnegie-Mellon University. CERT could be expanded into a wider forum for cooperation on specific vulnerabilities with participation by both government and private organizations.

The final area of potential engagement involves the somewhat sticky issue of information sharing between the government and industry over issues of information technology security. Stewart Baker, a former general counsel to the National Security Agency, highlights some of the difficulties of such sharing:

> Indeed, it's hard for government and industry to even have a dialogue on this issue. Five minutes into the discussion, industry says that it needs cheap unbreakable encryption to secure its systems, and the government asks how the FBI can catch the crooks who will use encryption to hide their activities. Ten minutes after that, industry is shouting "Big Brother" and the government is sermonizing about the World Trade Center bombing. By the time that fight has wound down, nobody has the energy—or the mutual trust—needed to discuss the gritty details of network security.
>
> And so we rock along, putting more and more of our infrastructure into cyberspace and hoping our adversaries won't notice or won't exploit those vulnerabilities. Fat chance.
>
> So far, the government's response has been heavily dominated by the military. But we won't get far without a consensus—one that includes industry—on questions like how we can identify organized attacks on critical civilian systems, how we can provide cost-effective protection against the most obvious attacks, and (as a way to get industry to the table) how to limit the liability of companies that act responsibly in reporting and protecting against attacks. (Baker, 1996)

Companies also have legitimate concerns about the sharing of proprietary or sensitive data. For example, banking firms are not likely to want their information security problems made public because of the possible impact on public confidence in the banking system. Likewise companies who are trying to sell a product would rather not have any security vulnerabilities with that product widely known for fear of losing business. Industry's fears are similar to military concerns about sharing classified or sensitive data with others. Breaking down these barriers in a manner that protects the legitimate interests of all will probably require government action to construct enabling policies and a legal framework for information sharing. Then more useful dialogue can occur on issues of concern to both the government and private sector and will help ensure that the military's dependence on commercial information technology does not become a liability as well.

V. FUTURE TECHNOLOGIES AND RESEARCH

> The first essential...necessary for our national security is preeminence in research. The imagination and inventive genius of our people—in industry, in the universities, in our armed forces, and throughout the nation—must have free play, incentive and every encouragement.
>
> — General of the Air Force "Hap" Arnold

Advances in technology have made available better and better information warfare capabilities. However, these advances have resulted from the reaping of research and development seeds sown years ago. What should be done now to ensure continued technological progress and greater information warfare potential in the future?

A. TECHNOLOGIES OF TOMORROW

Just as a previous question asked about the current enabling technologies of information warfare, this query seeks to project that same topic into the future. Although predictions of the future are always a dicey proposition, Delphi participants were asked to give their best forecasts on upcoming key information warfare technologies.

1. Delphi Responses

[Moderator] What are the future enabling technologies of information warfare?

[Campen] Again, it's not so much technology as it is the human-machine interfaces that allow us to exploit technology.

[Cochrane] Increased computer processor capability enabling rapid development of artificial intelligence and chameleon or polymorphic software which will hide its true identity and purpose.

[Cohen] Information technologies? This emphasis on technology is the wrong way to build the long-range future. The emphasis should be on understanding. De-emphasize systems, concentrate on concepts.

[Dunnigan] Common sense and respect (and detailed knowledge of) for what has gone before.

[Garigue] Easy high-level, end user programming capabilities will become essential as they permit rapid development of new information warfare and decision support programs. Being able to build a program will help users respond rapidly to new and emerging information needs. Visual programming, distributed software objects, scripting languages, and modular software will enable the user to rapidly enhance his information environment with new programs. So whatever new process is required it can be built by the end user himself. This will also shorten the time between requirements, specification, and development.

Also, as we will be faced with much more information than before, we will need to develop new types of knowledge management tools to monitor, collect, assess, filter, and aggregate data into information. Faster and more sophisticated clustering and classification techniques are required. Natural language interpretation and understanding based on cognitive modalities will help the query processes and enable a more useful dialogue between the human and the computer.

As information becomes more complex, there will be a requirement for high end visualization. Visualization permits greater transfer bandwidth between the human and the computer. Simulation will be integrated and continually used in all training and planning processes. Virtual Reality will also permit visualization as well as enable full sensory interaction with all types of data and information. VR will also play a significant role in support of individual and group decision support environments.

[Gust] Clearly, the expansion into frequency ranges using gigahertz as the unit of measure is the future. The existing and limited size of lower HF, VHF, UHF bands demands this extension. The technologies that will make the use of higher frequencies possible, like the millimeter wave solid state devices of today, need to be exploited.

[Hazlett] Offensive: jamming, global positioning systems, satellites, computers. Defensive: crypto, stealth, computers.

[King] Semiconductors (processors), optics (communications), cryptology, machine learning algorithms, data mining techniques, visualization, simulation of very large complex systems.

[Probst]
- programmable petaflops computers
- high-performance virtual networks
- high-confidence systems
- software infrastructure for high-performance data assimilation and analysis
- optical stores and interconnect
- directed-energy weapons
- ubiquitous information security including strong cryptography
- advanced modelling and simulation technologies

- unconventional man-machine interfaces (e.g., personal interfaces)
- also, the six Strategic Focus Areas of the CIC [Committee on Information and Communication] for HPCC [High Performance Computing and Communications]

[Schwartau] Uh uh! That comes out in IW2. I must be circumspect here. :-) [Note: IW2 is Mr. Schwartau's forthcoming book].

[Steele] Education of the individual from birth and continuing through their entire life.

2. Commonalities and Differences

First, a number of participants made the point that technology should not be the focus of any future thinking in information warfare. Emphasis instead should be placed on understanding of information warfare concepts, education of individuals and on the interface between users and advanced information warfare technologies.

Of those who took the question at face value, in general one could divide the answers into two types—physical advances and conceptual advances. First are the physical advances[1], which would include progress in the generic area of "hardware" technologies:

- Vastly increased computer processing capability
- Technologies to support gigahertz range frequencies
- Optical stores and interconnections
- Directed-energy weapons
- High-end visualization (virtual reality) and unconventional human interface tools
- Satellites (including global positioning systems)

[1]Interestingly, none of the participants mentioned microelectromechanical (MEM) systems or molecular nanotechnology as key future information technology areas. Mr. Larry Lynn of DARPA referred to MEM as a "potential breakthrough technology" that promises to combine mechanical and electronic devices into single, very small systems (Lynn, 1995). And molecular nanotechnology, if even half of the predictions made about it come true, will have revolutionary impacts on information technology in general (Drexler, 1991).

Second are the conceptual advances, which would include better methodologies, processes and "software" technologies:

- End-user programming capabilities
- Cryptology
- Machine learning algorithms
- Advanced modelling and simulation techniques
- Stealth (not the physical type)
- Knowledge management tools (data assimilation, mining and analysis)
- Polymorphic software

Finally, Dr David Probst mentioned the six strategic focus areas for high performance computing and communications put forth by the Committee on Information and Communications of the National Science and Technology Council. As recommendations that went directly into the President's budget submission, these areas deserve separate mention. They are:

- Global-Scale Information Infrastructure Technologies that build advanced application building blocks and widely-accessible information services
- High Performance/Scalable Systems to support "high performance" and "low end" applications in a seamless fashion
- High Confidence Systems that will provide the availability, reliability, integrity, confidentiality, and privacy needed by the Nation's emerging ubiquitous information infrastructure
- Virtual Environments and simulations that will continue to transform scientific experimentation and industrial practice, and will play an increasingly important role in education and training
- User-Centered Interfaces and Tools to provide easier development, navigation, "mining," and general use of information resources

• Human Resources and Education both to educate the next generation of industrial and academic leaders in information science and technology, and to establish a foundation for new learning technologies
(National Science and Technology Council, 1995)

B. SPENDING THE MILITARY'S R&D NICKEL

With the large number of potentially important future technology areas mentioned above comes the problem of where the military should focus its own limited and dwindling research and development funding. This question asks which of the key information warfare technologies or methodologies would merit military support.

1. Delphi Responses

[Moderator] Given the military's limited research and development funding, what specific research should it conduct? What specific technologies and methodologies should it support?

[Campen] Same as above. Study how to exploit the commercial technology to dominate your opponent.

[Cebrowski] We should be willing to apply a small percentage of overall R&D funding for pure research...divorced from a procurement tail. There are tremendous benefits of developing intellectual property that allows us a glimpse of future capabilities and trends without overstressing the current PPBS [Planning, Programming and Budgeting] system. (See response above)

[Cochrane] Secure distributed computing platforms, resilient public network infrastructures, automated software creation processes based upon a formally defined object structures, studies of complex systems including self organisation and auto healing techniques.

[Cohen] The question as put reflects on the thinking of the person asking the questions and in my view on the organization as a whole.

"what specific research should it conduct?"
"What specific technologies and methodologies should it support?"

Specific research seems to reflect research directed toward a specific (usually operational) need. In my opinion, we need non-specific research into information warfare. Understanding specific technologies and methodologies might be a useful result that could be derived from the research we should be doing. I think a good start would be to fund research into what long-term research results we will need to be effective in IW over the

next 20 years. I would be very happy to do this research, but so far, the only things I have seen accepted by the DoD as research projects are the development of systems to meet specific operational needs. In other words, military R&D is in a purely reactive and development mode—reacting to current needs and weaknesses by developing new systems—rather than a proactive mode—trying to understand what future needs may be and trying to understand what we don't yet understand.

[Dunnigan] People, in and out of uniform, who can do what has to be done. It's cheaper to cultivate the right people than to try and keep up with the commercial sector in spending. The money will not be there.

[Garigue] Security is paramount, so work on trusted-objects and trusted-processes is very critical to information warfare. Also new ways of clustering computers together to augment computational power and availability is important because one can then use low end technology to create high end computational networks that are survivable and flexible.

[Gust] This question needs to be asked of a combined arms team of users, researchers and materiel developers. One part of the community cannot answer this question alone.

[Hazlett] Realize that there are other parties with the same interests and start working with them, rather than trying to "go it alone." Where possible, team with other organizations, such as academia, and businesses. Where it is not possible, due to unique requirement(s), team with consistent allies, with like needs, such as Britain, Canada, and Australia. If it exists elsewhere, don't be afraid to buy it, or outbid others (it may be cheaper, in the long run).

[King] The emphasis should be on software and systems and not hardware. There are many research problems to be solved in the area of the effective, secure management of very large networks and systems.

[Probst] Two things:

- insist on programmable high-speed computers
- insist on virtual networks connecting distributed objects with bandwidth negotiation

[Schwartau]

- Insular technologies for mission critical commercial infrastructures
- Improved quality assurance
- Post-Information Warfare technologies

I have no doubt there's more, but I have a hell of a cold. :-)

[Steele] The military today in the U.S.A. is something like the military in the Third World (Luttwak's point) in that it is one of the last true national cadres of trained, disciplined, loyal people. If the military would stop lying to itself and others at the Service and ASD [Assistant Secretary of Defense] level, and share what it has learned about our vulnerabilities and gaps with the private sector, much of what we need would be developed at no cost to the government. Unfortunately, the areas where the military most needs development that will not be funded by the private sector is in the area of support to small Special Operations teams, and to the tactical commander dealing with

the 10 klick problem, and these are not massive sexy programs. The military should focus on "niche" R&D.

2. Commonalities and Differences

The first set of responses to this question addressed the generic approaches the military should take towards "spending its R&D nickel." In general, the military should focus on exploiting commercial technology by teaming with non-military organizations on items of mutual interest. For those areas of unique[2] military application, the U.S. military should engage in "niche" R&D in concert with traditional allied military forces in order to leverage combined resources. In addition, a certain portion of R&D funds should be focused on research not directed towards a specific application—so-called pure research into information warfare technologies and methodologies needed to be effective over the long term.

In terms of explicit technologies which would benefit from military funding, participants offered the following as candidates:

- Secure distributed computing platforms
- Resilient public and commercial network infrastructures
- Automated software creation processes
- Study of complex system characteristics
- Trusted objects, networks and processes
- Network and parallel processing computing
- Software and systems (vice hardware)

[2]Mr. Robert Steele succinctly makes the point that battlefield applications of information warfare of concern to such groups as Special Operations and engaged tactical commanders will not be of much interest to the general commercial sector. These areas would need some direct military funding.

• Improved quality assurance

• Virtual networks with bandwidth negotiation

C. OUTSIDE THE MILITARY-INDUSTRIAL COMPLEX

Engagement and interaction between the military and "traditional" defense companies (like Lockheed-Martin, Raytheon and Loral) has been on-going. However, many of the companies who deal in commercial information technology do not have a history of involvement with the military. Under the premise that such interaction would be useful, the next question asks how to conduct technology investment with such firms.

1. Delphi Responses

[Moderator] How should the military conduct technology investment programs with traditionally non-defense companies (like Sun, Microsoft, Motorola, etc.) who are now key suppliers of information technology?

[Campen] Probably not a cost-effective investment. Military has no leverage. Instead, take what they produce and learn how to run faster with it than the competition.

[Cochrane] See previous replies noting that robustness is also a high priority commercial issue. The development of an active aggression capability may well require traditional military funding.

[Cohen] The military should not be investing in those well-established commercially successful firms. Those firms can support themselves. The military should be putting out specifications for its long-range purchasing requirements to help guide the large firms that want to sell to the military so that they can make their long-term investments into the technologies the military will buy. The investment should be made in small high-tech firms and small high-risk high-payoff projects.

[Dunnigan] Don't act like know-it-alls. The non-military people have more experience at this sort of thing. Don't be lulled by stories of commercial firms that are clueless. There are always lots of those. Concentrate on the commercial outfits that have the goodies.

[Garigue] As we evolve our traditional command and control information systems towards coordination, communication, and cooperation of information systems, we will be relying more and more on commercial key suppliers to deliver all the building blocks the military

will use in support of defense and national security objectives. I believe that most of our present military information systems problems have already available solutions. For example, the recent "24 hour in Cyberspace" mission control (at www.sun.com—how did they do it?), has a lot of the same characteristics of an advanced Information Warfare command center. It had a DMZ [De-Militarized Zone], Clean LAN [Local Area Network], collection, analysis, and production centers, mirrored repository sites, and CERT [Computer Emergency Response Team] groups. The military will have to divest itself from not "invented here" syndrome so it can recognize ready made solutions. Future technology investments might not increase the information differential so much as an "Information Warfare Personnel" investment program.

[Gust] Key companies like Sun and Motorola have large divisions devoted to the government sector. They are coming to us.

[Hazlett] As if they were in it as a business—getting the most bang for the buck. Provide incentive or seed funding to lead R&D efforts in directions of government interest.

[King] I do not think there is any one answer here. One way is to cooperate with them in the funding of research at universities and research centers. It would be very useful to have more exchange of people between the military and these companies on rotational assignments but this is easier to talk about than to do.

[Probst] Be sensitive to investments in the margin. Look for future military-critical technologies in small companies.

[Schwartau] The model is the same as it is today. The Chinese Wall works. Look at the way that academia is handled. I don't see any conundrum here.

[Steele] In the IW arena, "non-defense" is an oxymoron. The military has one unique advantage in this era—its legitimate pre-occupation with security and survivability has made it sensitive to vulnerabilities and needs that are now essential for home defense and economic prosperity in the private sector. The military needs to teach rather than invest.

2. Commonalities and Differences

Several participants questioned the basic premise of the subject. They felt direct investment with commercial information technology firms might not be worth pursuing. Non-defense commercial firms are doing just fine without military help and in fact they are coming to the military to sell their wares without any technology investment funds. Instead the military should concentrate on articulating where its requirements are different from other customers, on investing in militarily unique items and on supporting small high-tech,

high-payoff companies with technologies that are potentially useful for military applications.

Finally, others made the point that investing dollars is not the only way to engage with non-defense firms. Programs to promote interaction, perhaps by expanding current efforts like "Education With Industry" to include exchanges with non-defense oriented companies and rotational assignments of business people into military groups, could do much to promote cooperation and an understanding of what commerce has to offer and what the military can use.

D. SYNTHESIS

Technology is a key enabler of information warfare capabilities. Advances in technology give the promise of even better information warfare capabilities for tomorrow. Such advances often stem from the research and development activities conducted throughout both industry and the government. With dwindling R&D funds, it is imperative that the military focus its efforts in ways that allow it to leverage research done in the commercial sector and by concentrating on uniquely military needs.

To do such focusing requires some sort of projection of the technologies that may be crucial for future information warfare. Delphi members listed many candidates in this area and gave some recommendations as to which ones the military should support. In a similar vein, a recent Defense Science Board summer study listed a number of specific information technology areas where the commercial marketplace is not likely to focus and that would benefit from military investment:

Technologies for Enhanced Reconfigurability
- "Component systems" development and evaluation tools
- Common reference models—digital terrain
- Self-describing data models
- Antennas
- Low-cost digital radios
- Dynamic information distribution
- Application specific data compression

Technologies for Information and Information Systems Protection
- Automatic classification downgrading procedures
- Tools for risk management
- Component level authorization, authentication & access control techniques
- Vulnerability models and metrics
- Failure detection, containment & recovery procedures
- Infrastructure protection mechanisms
- Classification management for data objects
- Data integrity techniques
- Data contamination recovery procedures

(Defense Science Board, 1994)

Likewise, the Air Force Scientific Advisory Board has also taken a look at technologies that the military (in this case, the Air Force) should support. Of interest, while listing specific areas for investment, the group also cited fields where the Air Force should stop doing research and development in an effort to focus investment monies on truly "niche" product areas. Some of their suggestions for technologies to stop focusing on include:

- Software development of software tools
- Mandatory use of Ada
- High capacity communications "backbones"
- Cryptography routinely embedded in systems
- Multimedia technologies
- Natural language understanding
- Computer displays
- "Information broker" software
- Basic directed-action software agents
- Software for "business" functions

(Air Force Scientific Advisory Board, 1995)

Besides looking at specific areas to support and particular efforts not to support, there is one additional way to look at the question of identifying the important information warfare technologies of the future. That is to describe the desired attributes of future systems and then to support militarily unique research that promote those attributes. For example (this is not an inclusive list), one might wish that the information warfare technologies of tomorrow be faster, smaller, robust, reliable, secure, fault tolerant, handle large amounts of data, and have a superior user interface. Working backwards from such a "feature set" can help to guide the R&D investments of today.

In sum, sowing the seeds for tomorrow's information warfare technology will mainly require that the military engage with the world-wide commercial sector for the technologies that will satisfy a large portion of military needs. An important part of this engagement will be "cross-fertilization" between the military and civilian worlds. One reason this cross-fertilization is needed is so the military can learn how the commercial world operates and what it has to offer. The other reason is for the military to communicate its own desires and needs to promote understanding of military requirements among the non-defense firms. Then the U.S. military (most likely in cooperation with allies) would then be free to spend its own limited R&D funds on "investments in the margins" to address novel military requirements that are not likely to be met by commercial developments.

VI. AN INFORMATION AGE ACQUISITION ORGANIZATION

> The prior acceptance and application of the thesis that superior arms favor victory, while essential, are insufficient unless the "superior arms" are accompanied by a military doctrine of strategic or tactical application which provides for full exploitation of the innovations. *But even doctrine is inadequate without an organization to administer the tasks involved in selecting, testing, and evaluating "inventions."* The history of weapons in the United States is filled with evidence on this point. [Emphasis added]
>
> — I. B. Holley Jr.

The movement of the military to embrace information warfare has already had obvious organizational impacts in the operational world. All of the services have established information warfare centers or activities, warfighting Commanders-In-Chief (CINCs) have developed information warfare cells and the Air Force is even in the process of standing-up an "information warfare squadron." This chapter seeks to explore whether military institutionalization of information warfare also implies the need for organizational changes in the development and procurement agencies.

A. ORGANIZATIONAL STRUCTURES

One of the traditionally key organizational issues is the debate between centralization and decentralization. Centralization usually offers tighter control, economies of scale and a more "top down" management approach—as well as a reputation for excessive slowness, bureaucracy and lack of innovation. On the other hand, decentralization offers the promise of a flattened hierarchy, more accountability and increased flexibility, at the risk of loss of focus and control (Daft, 1995). But with the advent of information technologies, an organization might be able to overcome any

problems of decentralization with robust communication between the various parts. Thus this question seeks in several different ways to explore the appropriateness of acquisition decentralization.

1. Delphi Responses

[Moderator] Should the procurement of information technologies be decentralized? Should procurement funds be given to the unified commands (e.g., Pacific Command) and/or individual units instead of the individual services (e.g., Army, Navy, Air Force)? Or is a "joint" acquisition organization (perhaps similar to the Strategic Defense Initiative Office) more appropriate?

[Campen] The framing of this question still implies a focus on THINGS. Information services should be established by functional basic ordering agreements that apply to similar functions in all services, on a global basis. Individual units then access these information services essentially the way they now do food and water, paying a users fee, if necessary, to support a common industrial fund. Using Intelligence as an example, DISA [Defense Information Systems Agency] provides the communications protocols and controls the network at the operational level; functional activities, such as DIA, NSA and CIA provide the functionally tailored information services, and the user taps into the system as required.

[Cebrowski] The spirit of Goldwater-Nichols and other mechanisms address these issues in that: a.) CINCs have more input in defining warfighting requirements—which is inherently decentralized b.) Operational units have significant latitude to apply discretionary funds in a manner that best meets their needs, and c.) The Joint Requirements Oversight Council ensures maximum warfighting efficiency by validating and articulating requirements to the Defense Acquisition Board—in essence, they embody the necessary ingredients of a joint acquisition organization. I prefer joint and decentralized to reinventing communism.

[Cochrane] Speaking from experience of a commercial organisation, decentralisation causes problems. A decentralised organisation results in a plethora of systems performing the same job in different location, on different platforms written in different languages. A centralised approach should provide a coordinated approach but needs to be fast and give the flexibility in the field. However, care must be taken to ensure centralisation does not bring the disadvantages of complete standardisation. If an organisation were to standardise on a particular type of hardware, it would be completely compromised if the hardware were to suffer a serious security breach. Are there any reasons for each service to procure information systems separately, let alone each unit? I would think that the needs of one type of military organisation are pretty much the same as the other. One absolute necessity is that the systems should interwork seamlessly. It would also be nice to think that a marine defending an army base should be able to use their equipment in the same

way as his own kit. If each service can not work with each other then the game could be lost before it starts!!!!!

[Cohen] Centralized planning—decentralized execution. The price and terms should be negotiated on a DoD-wide contract to minimize costs. The specific equipment should be ordered and processed by the most local person needing it. The acquisition should be based on an established need and method for fulfilling that need identified to and approved by the chain of command.

[Dunnigan] It already is decentralized. Lotsa luck separating the individual eggs from that omelet now.

[Garigue] The question of centralized vs. decentralized organizational structure is a big debate and an essential one. The money should go where the knowledge is. Who knows best should decide. Certainly the architecture and the standards could be centralized and the acquisition and the procurement can be decentralized. But in the case of very large organizations such as the Army, Navy, etc., the question cannot be resolved because all organizations have enough capabilities and resource to suffice to their own needs. None will agree on either solution. So the debate will continue.

[Giessler] Decentralized? Yes. Procurement funds given to unified commands and/or individual units? Yes for most I.T., only unique non-COTS stuff should be centralized. Is a "joint" acquisition organization more appropriate? Only for unique stuff and that should be less than 5 percent.

[Gust] We have had CINC-initiatives with discretionary funds for many years. It has resulted in some duplicative procurement and some non-interoperability horror stories. One cannot even specify UNIX without some disconnect across that product line. I think some centralization at the Service level is appropriate, mainly because that is where the best handling of funding and most flexibility in any reallocation or reprogramming of funds occurs. A joint activity carries too much baggage. My latest and most perplexing problem is to try to start a new common intell broadcast receiver program without a finalized joint ORD [Operational Requirements Document]. I have FY 96 dollars that must be spent, but the joint ORD approval process, which requires CINCS' coordination, will take so much time as to be in the next fiscal year. Jointness in buying JTIDS [Joint Tactical Information Distribution System], GPS, MILSTAR are three examples where time was traded for joint coordination, but Services retained the dollars on these programs. That is probably the best way to go.

[Hazlett] Should be more coordinated, not less. Particularly important from an affordability viewpoint. There is little overlap today between the services, even where there are similar, or even identical requirements. Virtual organization concept has merit in the acquisition world. Services, CINCs, etc., should form temporary virtual alliances when like needs exist, or joint development makes sense. One large acquisition organization may be too unwieldy.

[King] The goal should be to make the procurement process as efficient as possible. Something like a central group that prepares specifications and bid guidelines and then each command doing its own actual acquisition.

[Loescher] I would go further. ALL organizations, including tactical organizations, will be streamlined. Modern command is about moving information to take advantage of openings that happen orders of magnitude faster—and further from the tactical operations area—than war in the past. The officer hierarchy structure is a reflection of 19th Century land warfare and 20th Century ricebowls. With respect to development, a centralized, much smaller, Service-specific R&D outfit with ties to industry labs and Universities is the way to go, at least for the next 5-8 years. Government employees at the mid-level cannot stay in touch with commercial technology to buy it properly; but they can be focused on Service unique problems, which are not insignificant. Procurement of information systems should be decentralized; procurement of large information pools may be better bundled.

A joint office, just means, joint bureaucrats. What we need are new ideas to create new markets for new industry to sell to us—not more bureaucrats to oversee the existing industry, which is a reflection of yesterday's acquisition.

[Probst] Definitely, but interoperability can be guaranteed. But management gurus are not to be blindly trusted.

[Steele] Yes and no. Local authority over the realignment of funds is critical. For instance, PACOM [Pacific Command] briefed me several years ago that they had hundreds of thousands of dollars earmarked for TEMPEST hardware they did not need, and zero dollars for open source collection and production (including their library), so they had to cancel their LEXIS-NEXIS account. Generally the local command knows its needs best. HOWEVER, the current system of penalizing commands for savings is out of touch with human nature. They should be allowed to roll saving overs and reinvest in other priorities. Joint mandates of specific systems and software will produce results as dumb as the Marine Corps suite, where one word processor is mandated and purchased, and ignored Corps-wide, while WordPerfect is bought by hook or crook and is the actual Corps standard.

[Todd] Realizing the short term focus of the Unified Commands, the truly "out of the box" thinking has come more from technology push from the Services (stealth as an example) than from requirement pull from the Unified Staffs. Of course, I realize this is an iterative process and the integrated priority lists are of significant value to identifying what to pursue technology wise. Likewise, a joint office has its place in a very restrictive role. The Services should retain their function in the R&D arena.

2. Commonalities and Differences

There are two basic threads to this topic—the centralized versus decentralized issue and the question of a joint acquisition organization. In response to the first issue, Delphi members favored a "centralized planning, decentralized execution" approach. Such activities as procurement of information pools or services, development of convenient

contract purchase vehicles and setting of joint standards[1] and architectures would all best be centralized. While most of the actual funds to order products and information services should be decentralized to the level where the users possess the best knowledge of what is required. Then within a standard architectural umbrella, units or CINCs would be able to order what they need either from central purchase contracts or directly from the commercial world.

The second issue is whether a joint acquisition organization for buying information technologies would be appropriate or useful. The consensus was that joint organizations have a place for limited and specific purposes and programs. But in general, individual services should retain their functions of developing new military-unique technologies (the so-called "technological push") and of "equipping," albeit in ways that ensure interoperability with other services and allies. Such interoperability will mainly be assured by common standards and architectures—although it is unclear exactly who[2] would set these standards or develop the architectures.

Finally, Mr. James Hazlett brings up the idea of "virtual" acquisition organizations. Under this concept, individuals from diverse organizations (users, acquirers, contractors, different services, etc.) would come together to form ad hoc alliances to address specific

---

[1]A note of caution is required here. As one participant warned, one must be careful not to suffer the disadvantages of complete standardization, which can inhibit innovation, technological progress and competition. More worrisome, from a defensive information warfare perspective, is that standardization can make the overall system or network more vulnerable to a single type of attack, while a diversity of systems gives some inherent protection (Stoll, 1989). Probably more important than standardization of hardware or operating systems is an insistence on interoperability between different commercial products.

[2]One suggestion is that the Vice Chairman of the Joint Chiefs of Staff, via the Joint Requirements Oversight Council, should be responsible for developing an architectural "building code" (Defense Budget Project, 1995). Another possibility is the use of the Technical Architecture Framework for Information Management (TAFIM) maintained by DISA—which is designed to provide a single framework for DoD information systems (Paige, 1995).

needs or collaborate on individual programs. Modern information technologies such as video-teleconferencing, electronic mailing lists and the World Wide Web have enabled the creation of such entities and allow them to function in ways that are independent of normal time and space considerations[3].

B. UNIT-LEVEL ACQUIRERS

If the acquisition of information technologies is decentralized to levels closer to the user, does this imply the need for a new kind of expertise at the lower levels? Is someone—perhaps called an "acquisition technologist"—needed who has the skills to properly apply standards and architectures, buy the services or systems and integrate it all into a joint system of systems that supports warfighter needs?

1. Delphi Responses

[Moderator] Should "acquisition technologists" be put in operational units in order to quickly acquire and transition new capabilities?

[Cebrowski] This is more a matter of process and education than one of organization.

[Cochrane] Three options depending upon how you define information warfare.
- Moving operational people to the technologists would be far less dangerous for everyone involved. Technologists could get military requirements for systems in the same way that they acquire requirements for commercial systems. When getting new kit into the field I would think operational personnel would be happier learning from their peers who know the problems of operating in the field rather than suits from computer companies.
- As new information warfare technology can change the face of a battlefield within hours it may be necessary for IW units to contain not only acquisition technologists but also their own front-line research and development teams.

---

[3]So instead of a user in Korea having to spend travel funds to go to a program review in the United States, he could pull the review's briefing slides off a web site. Or if an engineer on the West Coast needs the opinion of a user in Europe, he can send an electronic message and not have to worry about getting up at 0500 to make a telephone call across multiple time zones. Granted, such vicarious interaction does lack the human touch, so there will still be times when travel is required for face-to-face meetings.

- Since information warfare creates a whole new battle field, cyberspace, it creates a need for people that understand warfare to work closely with technology gurus.

[Cohen] No. The person who actually needs a particular piece of technology should be able to go and get it if they want to, but it should be a pre-approved item or technology (except on an emergency basis) from a pre-approved source at a pre-approved price.

[Dunnigan] Put them somewhere out of the way so that the end user organizations can go get what they feel they need.

[Garigue] The logistics officer should be able to buy anything—putting it together is another issue. There needs to be a Information System Officer for that. With new technologies there are new classes of specialists that are required. In the navy we went from sail to steam, with this a new officer cane into the wardroom, then with electricity came another type of officer, now with software becoming the dominant war technology there will be the requirement for a new specialty in the military.

[Giessler] Yes—but that will happen when we select people who think and have an I.W. paradigm and educate them at NPS and AFIT [Air Force Institute of Technology] and all PME [Professional Military Education] at all levels. The Thrashers and Elams and Garcias are already the info science and technology officers and officials. All we need to do is get out of their way. And Comdr Loescher is leading that effort at USN headquarters.

[Gust] The Army still uses its TRADOC organization as the "user's rep" to consolidate requirements. The last thing we need is for each Army division to buy its own technology and then have to join up in a large force side-by-side like in Desert Storm. If you want it bad, you'll get it bad.

[Hazlett] Should stand up several joint and single service organizational and technological testbed units whose manning includes acquisition technologists. Not sure that they really belong or can be kept gainfully employed in regular operational units.

[King] I would centralize the technology part of this and distribute only the actual acquisition part.

[Loescher] In the current model—buying systems vs. commodities—we are wasting our money. Decentralizing acquisition to buy systems decentralizes wasting of money. We need to get our heads out of hardware and software and into information. We don't need acquisition technologists then, we need at new kind of operator, who understands infotech as the technology of modern warfighter. He/she needs to take their places beside the aviation, armored, strategic bombing, etc, innovators of the 1920s to lead us into a different kind of warfare.

[Probst] I think so. Maybe not an operational unit strictly speaking.

[Steele] Acquisition is NOT an arcane specialty that requires magic incantations and special knowledge. That is the OLD acquisition paradigm where convoluted formulas had to be learned over years of study and practice simply to stay out of jail. The new paradigm should rely on open market viability and common sense.

2. Commonalities and Differences

Perhaps the best summation of the Delphi members thoughts on this question is that what is required in the operational units are individuals who have an understanding of the promises and pitfalls of information technologies—perhaps "information technologist" would be a better descriptive term. The actual "acquiring" of information services or systems may be the easy part, with the true difficulties lying in the areas of understanding technology, defining requirements, proper integration and appropriate use. Such individuals must also serve in a "translator" function that takes the needs of the warfighter and transforms them into requirements addressable by information technology solutions (Allard, 8 March 1996).

C. ACQUISITION COMMUNITY FOCUS

Much of the information technology procured by the military today is available off-the-shelf from commercial firms. Given the relative ease of acquiring commercial products, does this imply a need for a change in where the acquisition community aims its own organizational efforts?

1. Delphi Responses

[Moderator] With the focus on use of commercial products, where should the military acquisition organization concentrate its focus? Research and development? Management of contracts and contractors? Integration of systems? Development of interfaces and architectures?

[Campen] Assuming we need but a very small one, its focus should be on architectures, integration and interfaces, and continuity of service.

[Cebrowski] It should focus on simplification, outsourcing, teaming with suppliers, and making itself as small as possible.

[Cochrane] There is no simple answer to this: well defined architecture and interfaces are essential for rapid systems integration and reliability. However, continuous changes in the battlefield can only be met with new technology provided from a well funded and broad based research programme.

[Cohen] No. Yes. No. No.

[Dunnigan] If you buy in sufficient quantity, you can have a partial production run modified to your particular needs. This is done all the time. But you have to act like commercial purchasing operations (i.e., efficiently.)

[Garigue] Acquisition organizations should focus on shorter acquisition cycles and rapid distribution.

[Giessler] Most of it should go away but that which is left should either be a demonstration center which shows off commercially available products and what will soon be available or it should be acquiring unique stuff. The acquisition field must change. Research and development? Not much here and most of this should be done across service if not at the JCS/OSD [Joint Chiefs of Staff/Office of the Secretary of Defense] levels. Management of contracts and contractors? Local user goes out and buys COTS and support necessary—that will be different for each user and may change when someone arrives, then leaves a job. Integration of systems? The local group will decide if they are competent to create interoperability and integration software, hardware, management ware, etc. If not they will hire it done for the 12 to 18 months before they buy new stuff. Some parts of their info system will always be changing by their COTS buys. Development of interfaces and architectures? The C.O. [Commanding Officer] has the vision and his people either develop or hire or buy the interfaces that will allow them to do the job with their constantly adapting architectures.

[Gust] I think the focus has to be on all frontiers, none at the exclusion of the others. We just have to be cognizant of what the other players are doing.

[Hazlett] Military acquisition organizations should concentrate their efforts on identifying those areas where the military can best benefit from economies of scale and on identifying and coordinating the management of cross-organization and organization unique needs.

[King] R&D to keep abreast of changes and development of interfaces and architectures in order to provide the acquisition guidelines.

[Loescher] The first two. There are many Service-unique or at least military-unique R&D problems that will never be solved in industry. Secondly, we need to create a process at the contracting level to capture innovation and to learn how to pay for information, which is different than paying for torpedoes.

[Probst] DoD does almost no research itself, and not much more development. DoD labs are quite different from DoE labs. Only options two and three are feasible.

[Schwartau] R&D for basic technology yes, in cooperation with the private sector, more along the European model. Standards are the key. I bet my bottom dollar that in a contest, a commercial outfit could get a system up and running much faster than a burdened military structure given the same tasking orders. The commercial folks would pick and choose available parts and glue them together for fast functionality. For military applications, a hardening step would be required, especially for mission critical life/death systems.

[Steele] There are always going to be some areas where the private sector simply will not support the kind of R&D that is necessary for unique military requirements. In the C3I area:

- Tactical document acquisition and digitization (such as rapid and rugged scanning of rough documents that are crumpled, wet, and hard to read; take on non-trivial pattern recognition problems

- Automated time and space tags on all multi-media information

- Build the bridges from commercial remote sensing platforms to the NRO/GPS precision points and then return the production of 1:50,000 combat charts with contour lines to the private sector- also build the bridges from commercial imagery through GPS/NRO to precision munitions already mounted on aircraft

- Digitize interactive speech for military police, coalition command & control, prisoner interrogation

- Communications & computing security

[Todd] The military should concentrate on integrating those systems deemed necessary to having a positive impact on the information battlespace. Knowing and having reliable information on our own forces; then being able to acquire, mix, synthesize and distribute information about our adversaries; then being about to orchestrate truly coherent operations against the enemy will have the greatest impact in future conflicts.

2. Commonalities and Differences

There was little convergence in the answers to this question. While there was a strong feeling that the role of the acquisition community should be small and simplified, the members split on what the exact focus should be. Some felt that conducting military unique R&D was a proper role, while others argued that the DoD really does little R&D itself and merely outsources research to others. Others felt that contract management would be a key activity of the acquisition community, but one member argued that local users should be

able to do this themselves. Likewise for the integration of systems and the development of architectures and standards. Several members thought these were proper functions while several more members said that the users could best integrate systems and develop their own architectures based on commercial standards.

Finally, Dr. Fred Giessler suggested that an appropriate role for the acquisition community would be to run information technology "demonstration centers." Such demonstration centers would highlight newly available or soon to be available commercial items so that the individual users have a means to keep up with the latest technology.

D. INSTITUTIONAL IMPEDIMENTS

Although not strictly an acquisition organizational question, this issue seeks to explore the existence and nature of any built-in obstacles to the development of an information warfare "infrastructure."

1. Delphi Responses

[Moderator] What are the institutional impediments to the creation of an information warfare infrastructure?

[Campen] Trying to adapt a structure built to buy, field, install, maintain THINGS into one needed to obtain information services. As the Congress noted in passing the new rules for acquisition of information technology, the hardest thing to change will be the culture.

[Cebrowski] The infrastructure already exists—what's needed is more time and effort for intellectual maturity.

[Cochrane] Impediments to the creation of an information warfare infrastructure.
- Military and governmental establishments and those that derive power from their positions in such organisations.
- The acquisition agencies with their preferences and cozy relationships with the "safe" traditional suppliers.

- Selling the concept to the public. If you say that there is a need for information security improvements the implication is that systems are insecure. No one wants to admit to problems, they just want to sort them out on the quiet, the result is that knowledge is not shared. The public are also quick to see a conspiracy and think that faceless governments are going to use the systems to further their own aims.

[Cohen] Were there any?

[Dunnigan] Stepping on someone else's toes.

[Garigue] The mind set. Cyberspace is not seen as a possible battlespace.

[Giessler] The most difficult is to get national security operatives at all levels to drop their old paradigms. The infrastructure is an implicit one that has to be inculcated not defined. It has to be part of the control system of individuals and organizations who understand the goals, objectives and CO's that capitalize on the COTS technologies—and then educate, train and exercise the force to create a revolution in military affairs.

[Gust] Everyone wants to be in charge. How many times have we have a new initiative and one Service has jumped up to lead so that their service-unique views or needs are served first? Examples are UAV [Unmanned Aerial Vehicles], strategic defense, space-related technology. We cannot all be the leaders, and the leaders have to be more accommodating of the needs of the other services. The followers also cannot be too parochial in their demands for "all or nothing" type solutions.

[Hazlett] Rice bowls and service rivalry, primarily. The services have been way too quick in carving up IW into narrowly defined areas. Some IW areas can best be handled in concert, rather than singularly.

[King] Information warfare is much more abstract than conventional warfare and it will be harder to get people to think about (and fund) it. In order to successfully control a networked nation it will probably be necessary to increase the security and therefore the restrictions. This goes against the current "open" atmosphere.

[Loescher] Institutions. You cannot create a new kind of warfare with old stovepipe warriors. But the stovepipe warriors control promotions—until we find a means to truncate the dynasties or until the dynasties tragically prove their unsuitability to the new world. Historical examples are everywhere, from the Trenches of WW I to Battleship Admirals to today's Information Warfare—which is basically cryptology reinventing itself in the guise of new term. There is a new Information Warfare, absolutely, but you won't get there by renaming the past, which is Navy's current mistake.

[Probst] Established privilege. Empire building. Lack of agreed-on concepts.

[Schwartau] I do not know what an IW infrastructure means here. I could interpret this a dozen different ways. Sorry.

[Steele] The institutional leaders below the Secretary of Defense. ACTUAL—the classification of the threat. The games Navy plays to compartment IW simply to keep its own toys and avoid joint endeavors. The general lack of understanding at the flag level of why intelligence is broken and open sources are a major part of the IW fix. The unwillingness of ASD C3I [Assistant Secretary of Defense for C3I] to stand tall and tell it like it is...

2. Commonalities and Differences

Several different threads emerge from the comments on this issue. First, that it will be difficult to adapt structures made for the acquisition of <u>things</u> into the structures needed to acquire information services. Second, that the military services have started to stake out narrowly defined portions of information warfare and are moving in directions that (naturally) serve service interests first—perhaps at the expense of the whole. Third, the sometimes abstract and ill-defined nature of information warfare makes it hard to articulate the threat in ways that garner support and funding from both inside and outside the DoD.

The last impediment mentioned is the possible resistance to information warfare from the current warfare-specialty stovepipes. The solution to this problem, as articulated by Dr. Stephen Rosen in *Winning the Next War*, is for leaders with traditional warfare credentials to support and reward those who would practice a new method of warfare—in this case information warfare (Rosen, 1991).

E. SYNTHESIS

Some of the inherent characteristics of information technology may make possible changes in the organizational structure of how information systems or services are acquired. A good analogy might be the current way telephone services are handled. Based on commercial standards, local users determine their own requirements and then telephone

specialists at the local level are free to buy, install and support their own equipment and services to meet the user's needs. There are obvious flaws to this analogy since there is currently no monopolistic "Ma Bell" to develop the basic information technology standards and it is not clear that this approach will scale well to the entire range of information technologies now available. But perhaps this model is a worthy goal. If a good portion of the technology is mature enough and if the standards and technical frameworks are available, then acquisition of specific information technologies can be "pushed down" to levels closer to the warfighters. Then systems will be seen more as "information appliances" and information services as no different than signing up for telephone service. Promoting the activities that enable this type of decentralization may be a key role of the acquisition world.

Such activities would include the continuation of R&D for military-unique issues, support for the development of both DoD[4] and commercial standards and architectures, development of convenient contract purchase vehicles and the demonstration of new technologies as a way to educate users as to what is available. The organization to do this may not be that structurally different from today, although it might be greatly simplified and streamlined. Instead, it may promote and lead ad hoc alliances to address specific needs or collaborate on individual programs using modern information technologies such as video-teleconferencing, electronic mailing lists and the World Wide Web.

All of this decentralization implies a need for individuals with greater expertise at the user level in order to acquire, integrate and sometimes operate information technologies.

[4]The development of DoD-wide standards and architectures (partially based on commercial standards) will be key to avoiding interoperability problems between the services and commercial entities.

Mr. James Hazlett and Dr. Martin Libicki call these individuals "information warriors" and they recommend the following as required areas of expertise:

> The information warrior must know not only programming but systems integration and system theory, communications, security, artificial intelligence, logic in all its many forms (classical, fuzzy, and convergent), and statistical techniques. The information warrior must also know the customer's needs: the commander's intent, doctrine, and strategies. (Hazlett & Libicki, Autumn 1993)

Given the broad range of expertises listed above, growing individuals with even some of these skills looks to be a difficult task. While many of these competencies have been the purview of users (i.e., understanding the commander's intent, doctrine, etc.), others have been more traditionally associated with engineers and scientists, the bulk of which are located in the acquisition and research organizations. Most likely such "information warriors" will be drawn from both talent pools to accomplish the tasks of acquiring information services or systems, understanding new technology, translating the needs of the warfighter, defining requirements, and integrating systems into a larger whole.

Finally there is the question of "institutional impediments" to the development of information warfare capabilities. Chief among these may be the bias towards the one-time procurement of large systems designed over years and expected to last over years and sometime decades, as opposed to the incremental development and enhancement of smaller systems and the procurement of information services (Loescher). Colonel Ken Allard of the National Defense University lists several others in a recent article where he talks about "living up to [the] technological promise" of information warfare:

> Although the defense budget is the most obvious constraint, there are other institutional impediments as well. Among them: the continuing struggle to temper the services' tendency to pursue separate modernization paths and the parallel need to rationalize the 5,000 separate C3 systems current operated by the DoD. Not only are these systems expensive, they are a form of self-inflicted information warfare whenever we conduct joint operations...Further acquisition reform is a related challenge. While significant improvement in commercial-military integration have been enacted, their implementation through the FAR has been slow. And it may well take a generation to product a defense acquisition work force skilled in sophisticated surveillance of the commercial marketplace and capable of entrepreneurial risk-taking. (Allard, 4 March 1996)

Progress in all of these areas will doubtless be slow given the nature of large and sometimes competing institutions. In addition, several of these impediments are more procedural than organizational, and will be examined more in the next chapter.

VII. CHANGES IN THE ACQUISITION PROCESS

> The survival of nations or even of whole cultures may depend upon the ability to procure superior weapons. It behooves us to be certain that our system is adequate to ensure this superiority.
>
> — I. B. Holley Jr.

Acquisition of weapons has long been an important part of a nation's military strength. Even the ancient Greeks recognized the importance of "acquisition." In Greek mythology, a separate deity—Vulcan—was dedicated to the development of tools for use in war and it was his task to forge the lightning bolts for Zeus to use in conflict. Today, raw information warfare technology must be developed, acquired, or "forged" into a form useful to current warriors. But do the defining characteristics of information warfare imply changes in how the U.S. should acquire or "forge" information warfare services and systems?

A. CYCLE TIMES

One of the traditional criticisms of the acquisition system is that it takes far too long to develop and field advanced systems. Lags of years between program initiation and start of field delivery are not uncommon (Dupont, 1996). These lags can result in military systems that are far less than cutting edge. This problem is exacerbated by the rapid pace of information technology development, which coupled with generally widespread commercial availability of such technology, creates the danger of potential opponents "getting inside our acquisition cycle" when they are not constrained by a formal

procurement system. This questions probes how the acquisition cycle might be speeded up to avoid such a situation.

1. Delphi Responses

[Moderator] Given that new generations of commercial information technology come, by some accounts, every 18 months, how do we address the need for a quick acquisition cycle time?

[Campen] We begin by abandoning the term "cycle," or at least redefine it as an open-ended, never-ending series of cycles. Also, we rid ourselves of the obsolescent concept that we are "buying a system." It has been almost 20 years since an AFCEA [Armed Forces Communications and Electronics Association]-run study coined the phrase "evolutionary acquisition" in an effort to make the point that there is never a Final Operational Capability, only a series of buy a little, test a little increments. The DoD Authorization Act of 1996 (HR 1530) makes some useful changes by focusing oversight on the function of an organization and the outputs to be gained from new information technology, and by urging "modular, incremental" procurements of "information technology." But that is not nearly enough for the U.S. to avoid being technically leap-frogged by adversaries that are not crippled by machine-age procurement regulations and cultures, nor burdened with an enormous investment in obsolete legacy systems. I think Navy Commander Loescher is the one to credit with the notion that we no longer procure information systems; instead, we acquire information services. (My words, his idea). We need to visualize the continuous enhancement of information systems in much the same way that we do software upgrades. We know there is always a software revision on the horizon and we program funds accordingly. The Block approach to aircraft upgrades is a step in this direction, but it can't be done if each increment must be refought with the Congress annually. We don't approach Congress with a line item to purchase electricity or water and we ought not need one to purchase INFORMATION SERVICES.

[Cebrowski] Spirited debate surrounding DoD Acquisition reform is not new. However, the strategic environment has changed so significantly since the inception of the current acquisition system that modernization is clearly warranted. A revitalized acquisition system that can keep pace with market forces is the surest way to maintain the most modern weapons systems. The focus should be on capabilities, not systems. The strategy should be one of continuous incremental technology insertion.

[Cochrane] The characteristics of information warfare dictate that a new software or network tool can provide battlefield advantage within hours of its conception. Therefore the research, development and supply chains will require re-engineering to suit. Commercial information technology may go through a generation in less than two years but changes in the fundamental platform and network architectures are much slower. Possession of the very latest technology will be critical to front-line Information Warfare units. More conventional units with less pressing needs could easily be supplied by normal commercial processes. Above all the growth in computing ability has to be allowed for when designing systems and then factoring extra security on top to be safe.

[Cohen] New IT doesn't often mean new underlying uses or techniques—they come far more slowly. Furthermore, for the first 6 months or so, any environment is unstable. The strategy should be to seek out more stable environments for conditions where long-term results are desired—hence you go for Unix and MVS and VMS and other stable environments as opposed to DOS and WINDOWS, etc [Note: these are all different types of computer operating systems]. Furthermore, re-acquiring technology every 18 months is not cost effective. Seek out technology that will last for 5-8 years and build on the more stable base. Abandon the reckless approach in favor of the more solid one. The exception is in experimental environments, where the state-of-the-art should be tracked, and in special cases where a really new capability enables advantages that are so significant that they warrant the extremely increased likelihood of failure associated with new technology.

[Dunnigan] Go commercial or die. Your likely future opponents will not have a military-industrial complex and will automatically go commercial and have the latest stuff.

[Garigue] Our present notion of information system delivery is outdated. We do not deliver systems anymore, we "grow" them. The present maturity of IT permits an organization to adopt a "technology insertion" strategy rather than a system development strategy. As new generation of network components are made available we can insert them readily into existing networks and IT infrastructures. We introduce these components in a prototyping context.

The focal point however is not just on managing the technology but on managing the functionality. As functions have a longer cycle than technology we must ensure that we outline a migration of the stable functions embedded in older technology to the new ones. We must also ensure that such a migration path will ensure the minimal amount of disruption of service over the course of the transition. This way, over time, older technology elements of a network are replaced by newer ones and functions migrate from older hosts to newer ones.

[Giessler] Adopt USN [U.S. Navy] initiative and SECDEF [Secretary of Defense] dictate that COTS is standard unless otherwise strongly justified.

[Gust] We have now begun in the PEO [Program Executive Officer] world an earnest reduction in cycle time. RFPs [Requests for Proposal] are shorter, with fewer CDRLs [Contract Data Requirements List], minimal MILSTDs [Military Standards] for such items as comm waveforms, interoperability, etc. Contract negotiations are now including an oral discussion cycle instead of lengthy IFBs [Invitation for Bid] exchanges of written questions and answers, etc. But still if the new technology cycle is 18 months, we have to do more. One initiative is the POM [Program Objective Memorandum] wedge for unidentified new initiatives. Our Army Chief is asking the Congress for $450M in a wedge to buy the mature, value-added successes from the digitization demo. Another is for the Army TRADOC [Training and Doctrine Command] community to emphasize a reduction in their requirements determination cycle. There are still areas where we can reduce time.

[Hazlett] Lean toward software, vice hardware solutions, ensuring that hardware is easily upgradeable, taking advantage of more powerful chips and faster memory. Go to more modular systems.

[King] First, it is not necessary to always keep up with every new wave of products which is more alike every six months. Second, long term contracts should be developed with vendors who can provide upgrades and new systems over the life of the contract in an efficient manner.

[Loescher] There is a logic set here that we are missing consistently. The InfoTech industry, at this moment, appears to be growing much like the oil industry, automobile industry, power industry, and other markets initiated by broad change in technology. A global infrastructure is being built as the market for goods increases. We are still in the stage where the industry is dominated by engineers, who are attempting to sell specific products. It is analogous to trying to sell spark plugs instead of cars. Gradually, however, the market is becoming one of commodity and service—America Online, Netscape, Java, are all examples of the coming service market. In the future, I would bet acquisition time will become irrelevant—because we're not going to "acquire" it, we're going to buy information services and information itself as a commodity. Acquisition won't matter—C4I is dead; we'll be transitioning to the direct use of information itself, not building information systems, which will all be commercial—and perhaps common to the foe and the friend.

[Probst] Use ATDs [Advanced Technology Demonstrations].

[Schwartau] In basic COTS PCs this is true, but integration of complex systems requires greater development and testing time. The key here is platform and O/S [Operating Systems] standards, backward compatibility and an acquisition awareness that what is RFI'd [Request for Information] today is obsolete by the time the buy occurs. I would examine acquisitions which permit the upgrade of systems performance to current standards as of the date of purchase.

[Steele] Functional standards (as opposed to fixed standards), and true openness and inter-operability, are critical. HOWEVER, also critical are the identification and legislation of standards of security and other basic forms of functionality which must be embedded in all civil communications and computing capabilities in as much as 95% of DoD traffic goes over same. It is NOT possible to BUY what we need. It is only possible to LEASE, TEMPORARILY, civil capabilities in this area. The real progress will come not from firewalling internal unilateral systems, but from raising the generic security and capability of the ENTIRE global network.

[Todd] In the past, the U.S. military has done a dismal job of integrating information systems. That, however, has been a blessing in disguise in that our "system of systems" have not been susceptible to contamination (either malicious or accidental). But future systems should be easier to integrate and as such, we need to ensure these systems while acting independent are yet able to communicate among them (linked). Fully integrated systems may be like a house of cards and if attacked, not degrade gracefully.

2. Commonalities and Differences

The general answer to this question is that one should no longer worry about the acquisition of systems. Instead the focus should be on managing the functions[1] that make up the system and on the information services that are required by the user. For the former, technology upgrades should occur by an evolutionary "growing" of the overall system by migrating functions hosted in old technology to newer technology. In essence, there will be a continual insertion of technology such that the underlying system is never procured and disposed of in the traditional manner[2]. As for information services, there may be more of a reliance on the commercial world to develop the information delivery infrastructure and the role of the military will be as "content providers" for its own unique information requirements.

One other point deserves special mention. As one participant commented, perhaps the current cycle time is not that long given the nature of the task. While specific technologies may be changing every 18 months, the integration of complex military meta-systems does take more time—just as similar civilian information technology meta-systems are not built in a day.

B. THE SOFTWARE EDGE?

In the previous topic, several participants mentioned that concentrating on software solutions (instead of hardware solutions) and on leasing products (instead of buying

[1]Functions will be much more stable than the underlying hardware and software used to implement them.

[2]All of this presupposes common functional standards, a certain amount of backwards compatibility and an open, modular meta-system architecture that does not yet exist.

products) would be good ways to keep technology refreshed. Such suggestions are the focus of this topic and lead naturally to the next Delphi question.

1. Delphi Responses

[Moderator] Should there be a shift from hardware to software orientation in development? Should we lease hardware and concentrate our efforts on incrementally improving software?

[Campen] The functionality comes from the software; the hardware will provide the bits and the bandwidth accordingly and automatically. The emphasis should be on the leasing, acquisition or rental of information services, with each new increment improving functionality, speed, accuracy, security and reliability.

[Cebrowski] Warfighting requirements will always dictate development decisions while economies prevail in decisions to lease or own. Advancing technology itself has hardware and software on a natural collision course—neither will dominate, instead both will fuse into mutual dependence. The more important question is how to shift funding and management attention to the requirement and design phases rather than waiting for problems to become big and intractable.

[Cochrane] The split between hardware and software is somewhat arbitrary: you cannot divorce them in this way. (Why should you trust hardware more than software? There could be just as many problems in the silicon—storing away keys which are picked up by a "maintenance" visit for example) We must always consider the whole system, stop looking at elements in isolation, concentrating on reducing the time taken to develop integrated hardware and software solutions.

[Cohen] Leasing hardware is an extraordinarily poor investment. It's almost always better to buy the hardware and convert older systems for less than state-of-the-art uses. For example, even a 5-year old PC is still perfectly capable of being used for office automation functions.

[Dunnigan] This has already been going on.

[Garigue] We should buy hardware like we buy food. So that it can be consumed rapidly (if you don't it goes bad very quickly). Software on the other hand are the functions that are required whatever the hardware. Software is the essence of the system as it represents the processes required to support the decision maker. Computers are consumable. Most of the critical components of the network are already in the commercial sector anyway; what makes systems "military" are the fact that the tools and the technology are applied to military problems.

Software itself is being modularized and becoming more and more generic. So there is an opportunity to take advantage of this and tailor some systems to our needs. The point in all this is to know when our requirements for timeliness, pertinence, accuracy of the data cannot be meet by the existing components and to custom design our own solutions.

[Giessler] We should not be developing either hardware or software in the military or the national security establishment unless the commercial market is not meeting our needs because there is insufficient profitable demand. Even our interoperability needs should be met by commercial interface packages.

[Gust] We in the Army night vision business have a unique incident that we are working. During Desert Storm we bought an overstock of Generation I tubes that are now obsolete. Since we have moved on to Generation II FLIR [Forward Looking Infrared] technology, can we salvage any of this "sunk cost"? The answer is we may have found a way to sell back to the contractor the older versions for their direct sale to other customers, then receive credit on the contract to buy new Generation II devices. Lease of hardware is probably a better option for a weapons platform of less dubious value, like a truck. Every system the Army is buying now is specifying the Common Operating Environment and Army Architecture standard version 4.0. This is a flexible format conducive to the use of software upgrades as a process for insertion of increased capability.

[Hazlett] Yes, we should shift to software solutions where possible, leasing and outsourcing hardware where possible. May need to develop "wrappers" or metaphors to deal with unruly or yet-to-be-developed components.

[King] Yes, in most cases, the emphasis should be on software but changes in hardware technologies need to be monitored.

[Loescher] We should concentrate on identifying and categorizing information families and let the commercial world worry about hardware and software. If the future, the intelligence communities will become less and less useful, though that may be their best kept secret yet. The best intelligence, especially for Information Warfare, is going to come from industry sources—much like it did in the early days of World War II. I'm not going to want to know what DIA thinks about Guatemala, I'm going to want to know what the Guatemalan information infrastructure is—that's not going to come from DIA, or NSA, or CIA, that'll come from the commercial sector that does business in Guatemala.

[Probst] The situation is more complex than that. In large part, DoD needs to use third-party parallel hardware and software. DoD also needs to articulate the parallel hardware and software at the margin that will not be available elsewhere. Certainly the bulk of DoD time will be spent in writing defense applications, taking advantage of reuse wherever possible.

[Schwartau] Software must be improved in two ways:
- Quality of testing and reliability through the use of better automated development tools.
- Standards for platform migration will alleviate the constant need for total redesign every time a new hardware widget comes along.

[Steele] Not hardware, not software, NOT EVEN DATA COLLECTION. Our focus should not be on technology, except in-so-far as we mandate certain standards of performance, but rather on "intelligence," meaning; what information can be discovered, discriminated, distilled, and disseminated to the commander so as to enhance mission fulfillment? Taking SPOT Imagery as an example: it is not necessary to mandate anything other than the fact that we need 1:50,000 with contour lines and precision points (either GPS [Global Positioning System] or NRO [National Reconnaissance Office]...).

2. Commonalities and Differences

While there was some disagreement, there was also a fairly strong feeling that, in general, software should be the focus of military development efforts. This was caveated with the notion that most of the software and hardware necessary to meet military needs will still be available commercially. Thus any software development sponsored by the military would be only for those unique applications that embody the particular functionalities needed by the military and not available in the civilian world. Operating systems, system utilities, network services, etc. would all be commercially based, while some of the applications that sit on top of such a "common operating environment" would be specially-developed programs.

Commercial hardware, on the other hand, is inherently more generic and the prime consideration is keeping up with technological improvements since hardware seems to become obsolete fairly quickly (much quicker than the functions embodied in software). Thus hardware should be thought of more as a "consumable commodity" that must be used and replaced rapidly, either at the end item level or at the "board" level if the item is modular and flexible enough, while mission software, if it is modular, portable and reusable, can migrate from older hardware to newer hardware.

The second part of the question deals with the idea of leasing as a means to keep hardware current. An old business saw states "buy items that appreciate, lease items that depreciate." There was no clear response from the Delphi members on whether the idea this statement embodies is true and whether it is applicable to DoD information technology hardware. Some were flatly opposed to leasing, some felt it was the way to go—especially

for "commodity" hardware such as workstations and personal computers, and others felt it should be a purely economic decision made on a case-by-case basis.

Finally, both Col. (Ret.) Al Campen and CDR Michael Loescher thought the emphasis on hardware and software was misplaced. Instead, they argue for a concentration on acquiring or leasing information services. Under this view, worries about keeping hardware and software current would logically be left to the commercial world.

C. TECHNOLOGICAL OVERHANG

In the past, technologies instrumental in RMAs have often been developed in the civilian world and then "imported" by the military for warfighting purposes (Krepinevich, Fall 1994). With the slower pace of earlier technological development, there was usually plenty of time for the military to recognize, exploit and integrate such new technologies. But with the current rapid rate of development, there may be militarily useful information technologies that are not being recognized, exploited or integrated, thus creating a "technological overhang" of commercial information technology over currently fielded military technology. This question seeks to deal with how the military should recognize and "spin on" information technology innovations from the world of commerce.

1. Delphi Responses

[Moderator] With an increasing array of new commercial information technologies, who should be responsible for finding these new capabilities and how should we conduct commercial-military integration?

[Campen] The user, not some surrogate electronic arsenal attempting to craft a formal ROC [Required Operational Capability]. The Air Force Fort Franklin shows the way by providing an environment for experimentation, testing and functional demonstration.

[Cebrowski] The technologist must inform his potential customer, the operator—and operator must inform technologists. We shouldn't be concerned about commercial-military integration. The DoD should buy the 70-80 percent solution from industry; then reengineer business practices and requirements to make that a 100 percent solution. We can't afford otherwise.

[Cochrane] Integration is the wrong approach. Ordinary commercial organisations are becoming more aware of the need to have secure systems and therefore demanding the same strength as military products. If the military were to specify their needs at an early stage the commercial systems would be developed to the military requirements. This would produce economies of scale, reducing the costs of military systems. The military would no longer have to identify the capabilities of systems they were getting because they specified the capabilities.

[Cohen] You might try having an advanced technology group in the DoD that constantly seeks out new and useful technologies and applications and forwards information on these new developments to the appropriate other groups for consideration.

[Dunnigan] Someone in the military, I hope...

[Garigue] All organizations need to be doing some type of technology assessment activity. Comparing the recent developments in the commercial world with military requirements in test laboratories and doing technology insertion proof of concepts are a good way to "test and try."

[Giessler] The ultimate user should find the acquisition with the aid of people at places like NRAD, ESC, NRL, ARL [Note: these are all military acquisition or research organizations], service labs and academic places like NPS. This is going to be the toughest part...How to stay current and adapt/adopt/acquire/find/be aware of the available and useful technology. JWIDs [Joint Warrior Interoperability Demonstrations], Ft. Franklin, and ACTDs [Advanced Concept Technology Demonstrations] etc., will have to be used as well as displays at shows and conferences. We may find that we have to put DoD people out in industry just so we can keep abreast of what is going to be available. It may require a new specialty officer called the information science and technologist.

[Gust] The responsible party should be consensus forums, not single function activities like ARPA [Advanced Research Projects Agency], laboratories or PMs [Program Managers]. Using ACTDs from the R&D community results in the follow-on program fund lines to have in them a source of leave-behind funding for O&M [Operations and Maintenance] commands to evaluate in the field for two years. Also, fund lines need a production wedge for those R&D initiatives that will mature shortly, i.e., those funded at a 6.3 or 6.4 [Note: these are different kinds of R&D monies] maturity level.

[Hazlett] Need to coordinate information management across the services and agencies. Take better advantage of economies of scale, like needs and like requirements.

[King] There needs to be a group that keeps up to date on changes and can understand which new items are worth incorporating into the existing systems. It is probably best to outsource as much of the actual integration work as possible.

[Loescher] I disagree with the premise. The "array" of commercial information technologies is becoming more and more homogeneous, as standards become valuable to the marketplace. Thus, an information system for MacDonald's in the future will be much like that for DoD—they'll just need different information in different times and places.

[Probst] Well-trained specialists with reasonable career paths.

[Schwartau] I have no earthy idea how to solve this. How about establishing a technology excellence center, a sort of government help desk, which is staffed to address questions from interested acquisition officers on what the latest and greatest is. This center should also track the real-world commercial implementation of advanced technology, most notably in the financial arenas. Why reinvent the wheel for the sake of job security?

[Steele] Let the free market work its magic. Our biggest enemy now is misplaced security constraints which prevent openness, and procurement constraints which give an advantage to beltway bandits skilled at paperwork rather than genuine innovators with something unique to offer. DoD cannot put its house in order by itself; the White House must offer an umbrella program, and a genuine Chief Information Officer network at Undersecretary levels, with real resource authority, or the Services will continue to protect pet rocks and "special arrangements."

2. Commonalities and Differences

There was an almost general consensus[3] among the Delphi members on the question of keeping up with new technologies. First, participants felt that keeping up with commercial technology requires a partnership between the users and the technologists. The users possess a better understanding of operational requirements, while not necessarily having the time to keep up with technological developments. Technologists[4] have a sense of what is technologically possible and should be held responsible for keeping up with new

[3]CDR Michael Loescher did disagree with the premise that an "increasing array" of information technologies are becoming available. He felt that common standards are driving the commercial world towards more "homogeneous" products. While this may be true for product lines that are maturing, it is unclear if this is true for the "cutting-edge" technologies that represent new or unique applications of information technologies.

[4]These technologists could be from the service research labs (e.g., Army Research Lab, Naval Research Lab, the Air Force "Super Labs" like Rome Lab, etc.) and acquisition centers (e.g., the Air Force's Electronic Systems Center , the Army's Communications and Electronics Command, etc.), as well as from organizations like the Defense Information Systems Agency (DISA) and DARPA.

innovations. Working together, via such mechanisms as test beds, technology insertion programs, interoperability demonstrations and ACTDs, new commercial information technologies can be adapted, exploited and integrated into military units.

D. INFORMATION TECHNOLOGY LOGISTICS

Much of the Delphi discussion has focused on the development, acquisition and fielding of information technologies. However, just as important is the sustainment of those fielded technologies—the logistics support of information technology. This question asks how such logistics might be different in a world dominated by commercial information technologies.

1. Delphi Responses

[Moderator] Given increased use of commercial parts, should the military rely more on the commercial world for its information technology logistics support? Will it be better to "throw away" a broken system and order a new one rather than maintain the capability to repair it?

[Campen] Don't get trapped by the definition of parts for broken THINGS. Other than a cheap, commercial, dumb, terminal in the field, that does nothing more than accept applets from a global information service supplier, there is nothing to repair. If the dumb terminal is broken, then throw it away. The main concern ought to be ensuring continuity of information services.

[Cebrowski] Generally, yes; but where that is too expensive, do something else like reassess the requirement.

[Cochrane] See previous question. Presume that by "broken" you mean breached security. I would say the "new or repair?" question probably needs to be reviewed on a "per case" basis. However, it is probably safe to say that repair would be a valid option in many cases. The system breach might be fixed easily with little extra cost and with a good deal of confidence in the new level of security, without the worries of implementing a completely new system. If the replace option is taken it may be necessary to run the broken system until a replacement is available, this necessitates a certain level of repair. If a "broken" system were to be replaced it may be redeployed for use with lower grade information thus increasing its lifespan. It may be more economical to replace the infrastructure of the system with a new one.

[Cohen] Waste not want not.

[Dunnigan] The commercial model for operations stresses efficiency, thus it is the one to follow (as the military has done for centuries...)

[Garigue] There are no universal rules. The solution must be dictated by the problem and not a policy. In many cases there are good reason to dispose of systems in a rapid way. The fixed cost of repairing some components are not worth it. Better buy replacements. But new components sometimes come at the cost of poor backward compatibility and increased dependence on outside organizations.

[Giessler] Yes to both questions. And often we will throw it away because it is superseded—redistribution will replace maintenance.

[Gust] Actually, PEO-IEW [Program Executive Officer-Intelligence and Electronic Warfare] embarked on a "policy" several years ago that helps to solve this problem. We focused on 6UVME-formatted circuitry. This standard has turned out in industry like the VHS format in video recorders. With an open bus architecture, it is possible to plug in the next generation card and that is better than both repair of the old card or replacement of the entire system.

[Hazlett] The military should rely on civilian components except in those areas where there is no civilian equivalent, or there specific requirements that dictate a "military only" solution. Should go to more modular systems that can be incrementally upgraded, so that there are very few, true "legacy" systems. Upgrades to older systems often cost more over the long run, and provide less capability gains than new, replacement systems.

[King] For standard commercial systems, there are several vendors that can provide worldwide support. It is normally best to keep spare systems/components and switch to those while repairing the broken units. The repair versus throw-away decision should be based on economics.

[Loescher] It's better to do neither. We should lease the infrastructure and pay for it on our monthly "information bill."

[Probst] This is basically a question of outsourcing. If your source is competent, and will always be there for you, fine. Otherwise, watch out.

[Schwartau] That's a pure cost justification decision. Ask the commercial sector how it does it in comparable situations. Also, the IRS should change the depreciation of computer equipment from 5 to 2 years.

[Steele] It depends. On balance, because of the speed with which technology changes, it is NOT cost effective nor performance-mandated to protect legacy systems. In fact, they end up costing 80 cents on the dollar to maintain. However, there are going to be some elements that are not only critical, but too arcane for the private sector—and this leads to an interesting idea: if the private sector does not understand the value of a particular system, then either a) it really does not have a value and the military is overestimating its value or b) we should declassify the threat that inspired our value, and see if the private sector cannot adopt the same standards.

2. Commonalities and Differences

There were two threads to the overall question. First is the issue of whether the military should rely on commercial logistics support instead of building its own repair capability. The answers to this first query were very similar to the responses given to the question of whether the military should lease instead of buy. Many felt the decision to outsource logistics support to the commercial world should be made on a case-by-case basis depending on the particular costs and benefits.

The second issue involves the decision to repair or discard broken information technology items. Again, most felt this would be decided differently for each separate case. In those instances where technology is rapidly improving or the current system has little inherent flexibility or modularity to allow upgrades, then discarding the item and buying new would make sense. But if the technology would allow incremental improvements by software updates or board replacements, then repair (done either in-house or commercially) might make sense.

E. SYNTHESIS

Several broad threads emerge from this discussion. First is a consensus for an incremental approach to information technology acquisition, much like that recommended by the Armed Forces Communications and Electronics Association's (AFCEA) *Evolutionary Acquisition Study* (AFCEA, 1993). To keep up with rapidly advancing technology, there should be continual cycles of technology insertion via test beds, interoperability demonstrations, ACTDs and experiments[5] such that the underlying system is never procured and disposed of in the traditional manner. Key to accomplishing this incremental approach across a "system of systems" are implementation of standard data dictionaries, object-oriented and modular designs and well-defined architectures and interfaces (Strassmann, 1994). Also critical to the selection of which technologies are ready for incremental insertion is a partnership between users who understand operational requirements and technologists who are responsible for staying abreast of technical advances and opportunities. Finally, even such incremental improvement cycles can be sped up through the use of better acquisition methodologies. In this area the acquisition community should take a cue from operational users who are devising "distributed, collaborative planning systems" based on advanced information technology as a way to deal with the complexity and pace of the modern battlefield. For example, work is underway to move from a centrally-planned Air Tasking Order process that took 72 hours and was largely static, to a dynamic and distributed Air Tasking Order that is constantly updated and has a "cycle time" of perhaps six hours. Much the same may be possible in

[5]It is also important to note that such experiments be allowed (or even encouraged) to fail without the threat of instant program cancellation. Finding flaws quickly—before fielding—allows for early correction and promotes the risk-taking necessary for innovation and true "out of the box" thinking.

moving from a laborious acquisition planning and execution process to one that is characterized by responsiveness and constant interaction among users, developers, researchers and commercial firms.

Second, instead of focusing on the grand acquisition of "systems," the emphasis should be on managing the more stable functions that make up the systems and on the information services that are required by the user. In many cases those functions will be embodied in mission-unique operational software, the importance of which cannot be overstated[6] in a world where potential foes will have access to the same basic commercial hardware and software. A large part of any edge the U.S. possesses will be embedded in software and thus the focus of the acquisition organization should mainly be on development of the operational software and the integration of mostly commercial systems. As for information services, there will be more of a reliance on the commercial world to develop the information delivery infrastructure and the role of the military will be as "content providers" for its own unique information requirements.

Finally, decisions on leasing versus buying hardware, in-house versus commercial repair, and repair or discard issues will vary between individual situations based on the costs and benefits involved. Although the promise does exist of a greater move towards the treatment of information technologies as information commodities or information "appliances." Thus in many cases it may be cheaper and more effective to lease the information technology equivalent of a '96 Lexus for three years, only to trade it in on a '99 BMW when the Lexus starts to require more maintenance as it wears out and when the

[6]Squadron Leader Peter Emmett argues that "software is a weapon in its own right" and is key to combat effectiveness on a battlefield where most information warfare, C4I and weapons systems are dependent on its correct operation (Emmett, 1994).

newer BMW offers a qualitative and quantitative advance in performance. A similar situation may hold for logistics repair issues. If one buys a television and later has problems with it, it is usually cheaper to take it to a commercial vendor for repair. If the television is an older model that is no longer in production, it is often less costly to buy a completely new model with better capabilities than it is to have the obsolete model repaired. The acquisition and logistics system should be poised to take advantage of such possibilities whenever they exist.

One last issue deserves special consideration in terms of a specific impact of information warfare on the acquisition process. That issue is how product integrity and information warfare dangers are handled during design and development. In order to protect systems from information warfare risks, it will be important to ensure the systems engineering process includes up-front activities that assess critical areas and that take steps to mitigate information warfare threats to mission-critical system functions. The Air Force's Intelligence and Information Warfare Systems Directorate of the Electronic Systems Center has developed a comprehensive methodology to perform such an assessment. This methodology was recently applied to a major Air Force system that is in the operational test and production stages. The assessment resulted in a prioritized set of information warfare vulnerabilities and included specific actions the program director could take to reduce those vulnerabilities. Plans are underway to apply this methodology to several more programs still in the engineering and manufacturing development phase. This type of approach should be performed for all new or modified systems in order to explicitly address information warfare hazards. (Watters, 1996)

In conclusion, "acquisition reform" is an often-used and an almost institutionalized phrase in the DoD. Most Americans, both inside and outside of government, feel there are fundamental problems with the centrally-managed acquisition process and much effort[7] has been devoted over the years to the challenge of "fixing" the process. This chapter addresses just a few of the issues currently facing the acquisition world that have particular pertinence to information warfare and that are obviously closely tied to the more generic topic of information technology acquisition.

[7]While the acquisition establishment certainly is not perfect, much progress has been made in the past few years, some of it with direct applicability to the procurement of information technology. For example, among others items, the National Defense Authorization Act for FY 1996 repealed the Brooks Act (this repeal now gives agencies authority to directly purchase information technologies instead of going through GSA), streamlined information technology procurement procedures and included provisions for assessing the feasibility of leasing instead of buying (Crean, 1996).

VIII. SUMMARY AND CONCLUSIONS

> In the past, research and development were only preparation for the final and decisive testing of new systems in battle. Today the kind and quality of new systems which a nation develops can decide the battle in advance and make the final conflict a mere formality—or can bypass conflict altogether.
>
> — Bernard Schriever

At the conclusion of the initial Delphi process, Dr. David Probst remarked, "Our opinions are all over the map. No unifying theme has emerged." While this judgment may be accurate in terms of specific answers to specific questions, it is important to remember the purpose of this modified Delphi process. It was not designed to drive all parties towards consensus on all issues, but instead to facilitate a discussion aimed at generating a wide range of responses and ideas about information warfare. In this respect, this adaptation of the Delphi mechanism was a success, although back-and-forth dialogue between the participants was limited—probably due to the nature of electronic mail and the busyness of the participants. In spite of this, at least a few broad themes and specific ideas did emerge from the Delphi. These themes and ideas about the nature of information warfare and the impacts of information warfare on the acquisition system are summarized below.

A. NATURE OF INFORMATION WARFARE

As Dr. John Arquilla and Dr. David Ronfeldt state, information warfare has been around for ages in some form or another (Arquilla and Ronfeldt, 1992). But the modern

incarnation of information warfare is heavily based on the growing capabilities of and dependency on information technology. On one hand, information technology can be used to greatly enhance functions of society and warfare. But with such use comes dependency, that in turn creates vulnerabilities that may be attacked and must be defended. The process of attacking an enemy's information and information technology vulnerabilities for any political or military purpose and the protection of one's own information and information technology is the essence of information warfare.

The nature of information warfare is further delineated by the qualities of information technology itself—because the relationship between information warfare and information technology is deep and fundamental. While many methods of information warfare (e.g., propaganda leaflets and physical deception efforts) can exist independent of information technology, their effectiveness and usefulness can often be greatly enhanced by information technologies. There are also a number of modern information warfare methods that are completely dependent on information technologies. In general, these technologies[1] are the same for both waging offensive information war and for protecting against information attacks—only the techniques and applications are different. It also should be recognized that information warfare conflict has its own physical rules, logical rules and inherent limitations based on the unique traits of information technology. These limitations must be considered when conducting information warfare in a medium that some call "cyberspace." And with a few exceptions, such as electronic warfare platforms, there are not cleanly separable information warfare systems in the traditional sense. Much as C4I

[1]See Chapter III for a list of key technologies.

systems, information warfare systems are more collections of hardware, software, procedures and people[2] than discrete systems like aircraft, ships and missiles.

It is also evident that dependence on information technology is in large part a dependence on commercial information technology. The trend towards use of commercial information technology is profound and irreversible and such technologies will be largely available to all comers, reducing any purely technical edge to those few items that the military is able to develop itself and/or keep closely held. Thus to build any overall information warfare edge, it is important to properly adapt one's organization and doctrine and to accomplish the timely and correct integration, exploitation and synergistic application of commercial and military-unique information technologies[3]. This need to perform effective exploitation and integration, coupled with an increased use of commercial items, begs for better cooperation between the military and commercial sectors—especially in areas where military concerns coincide with the concerns of the overall market. Issues of product integrity, upfront consideration of security concerns during product development and the potential benefits of information sharing are all ripe areas for collaboration, although the mechanisms to promote such commercial-military teamwork have yet to be constructed in ways that take full advantage of the information age.

Thus part of any advantage in information warfare or any information warfare revolution is how effectively one can exploit and integrate new technology. Or said another

---

[2]In fact some argue that the best defensive information warfare investment one can make is not in software firewalls or hardware cryptological devices, but in enhanced "wetware" by giving systems administrators better training.

[3]These activities equate to the organizational adaptation, operational innovation and systems development steps of a revolution in military affairs. (Krepinevich, Fall 1994)

way, the characteristics of modern information warfare make one's information warfare edge depend substantially on how well one can develop, acquire and field new information technology. This leads to an investigation of whether the character of information warfare has specific impacts on technology research and acquisition activities.

B. ACQUISITION IMPACTS OF INFORMATION WARFARE

Similar to the steps of a generic revolution in military affairs, the impact of information warfare on acquisition can be probed by examining three different areas: technology, organization, and policy (or process).

1. Technology Development

Technology is a key enabler of information warfare, and advances in technology give the promise of even better information warfare capabilities for tomorrow. Such advances often stem from the research and development activities conducted throughout both industry and the government. But with dwindling R&D funds, it is imperative that the military focus its R&D efforts in ways that allow it to concentrate on uniquely military needs and to leverage research done in the commercial sector. To do such focusing first requires some sort of projection of the technologies that may be crucial for future information warfare. Delphi members, along with such groups as the Defense Science Board and the Air Force Scientific Advisory Board, listed many candidates[4] in this area and gave some recommendations as to which ones the military should and should not support.

[4]See Chapter V for lists of specific technologies.

Besides looking at specific areas, one can also describe the desired attributes of future systems and then support militarily unique research that promote those attributes. For example, one might wish that the information warfare technologies of tomorrow be fast, small, robust, reliable, secure, fault tolerant, handle large amounts of data, and have a superior user interface. Working backwards from such a "feature set" can help to guide the R&D investments of today.

Sowing the seeds for tomorrow's information warfare technology will also require that the military engage with the world-wide commercial sector for the technologies that will satisfy a large portion of military needs. An important part of this engagement will be "cross-fertilization" between the military and civilian worlds. One reason this cross-fertilization is needed is so the military can learn how the commercial world operates and what it has to offer. The other reason is for the military to communicate its own desires and needs to promote understanding of military requirements among the non-defense firms. Then the U.S. military (most likely in cooperation with allies) would be free to spend its own limited R&D funds on "investments in the margins" to address novel military requirements that are not likely to be met by commercial developments.

2. Acquisition Organization

Some of the inherent characteristics of information technology may also make possible changes in the organizational structure of how information systems or services are acquired. Instead of a centrally-managed[5] acquisition system, one may be able to move to a

[5]The centrally-managed acquisition system may be a major "institutional impediment" to the development of information warfare capabilities. The current system has a bias towards the one-time procurement of large systems designed over years and expected to last over years and sometime decades, as opposed to the incremental

more decentralized system where local users determine their own requirements and then information technologists[6] at the local level are largely free to buy, install and support their own equipment and services to meet their own user's information warfare needs. Of course this may be workable only if a good portion of the technology is mature enough and if the standards and technical frameworks are available which ensure interoperability. Then acquisition of specific information warfare technologies can be "pushed down" to levels closer to the warfighters where information systems will be seen more as consumable "information appliances" and information services as no different than signing up for telephone service. Promoting the activities that enable this type of decentralization may be a key role of the acquisition world. Such activities would include the continuation of R&D for military-unique issues, support for the development of both DoD and commercial standards and architectures, development of convenient contract purchase vehicles and the demonstration of new technologies as a way to educate users as to what is available. The organization to do this may not be that structurally different from today, although it might be greatly simplified and streamlined. Instead, it may promote and lead ad hoc alliances of users, contractors and others to address specific needs or to collaborate on individual programs using modern information technologies such as video-teleconferencing, electronic mailing lists and the World Wide Web.

---

development and enhancement of smaller systems and the procurement of information services.

[6]Such local level "information technologists" must know how to acquire information services or systems, understand the promises and pitfalls of new technologies, be able to translate the needs of the warfighter into technical requirements and ensure the integration of individual systems into a larger whole.

3. Acquisition Process

Several broad threads emerged from the Delphi discussion about needed changes or reforms in the acquisition process. These changes have particular pertinence to information warfare, but are obviously closely tied to the more generic topic of information technology acquisition.

First is a consensus for an incremental approach to information technology acquisition in order to keep up with rapidly advancing technology. There should be continual cycles of technology insertion via test beds, interoperability demonstrations, ACTDs and experiments such that the underlying system is never procured and disposed of in the traditional manner. Key to accomplishing this incremental approach across a "system of systems" are the development, adoption and implementation of standard architectures and interfaces (such as the Technical Architecture Framework for Information Management or TAFIM). Also critical to the selection of which technologies are ready for incremental insertion is a partnership between users who understand operational requirements and technologists who are responsible for staying abreast of technical advances and opportunities. Finally, even such incremental improvement cycles can be sped up through the use of better acquisition methodologies that make use of advanced information technologies to develop a "distributed, collaborative" acquisition planning and execution process characterized by responsiveness and interaction among users, developers, researchers and commercial firms.

Second, instead of focusing on the grand acquisition of "systems," the emphasis should be on managing the more stable functions that make up the systems and on the information services that are required by the user. In many cases those functions will be

embodied in mission-unique operational software, the importance of which cannot be overstated in a world where potential foes will have access to the same basic commercial hardware and software. A large part of any edge the U.S. possesses will be embedded in software and thus the focus of the acquisition organization should mainly be on development of the operational software and the integration of mostly commercial systems. As for information services, there will be more of a reliance on the commercial world to develop the information delivery infrastructure and the role of the military will be as "content providers" for its own unique information requirements.

Third, decisions on leasing versus buying hardware, in-house versus commercial repair, and repair or discard issues will vary between individual situations based on the costs and benefits involved. Although the promise does exist of a greater move towards information commodities where in many cases it may be cheaper and more effective to lease information technology or to discard an obsolete information appliance at the end of its useful life. The acquisition and logistics system should be poised to take advantage of such possibilities whenever they exist.

Last is the issue of how to promote product integrity and identify information warfare dangers during design and development. In order to protect systems from information warfare risks, it will be important to ensure the systems engineering process includes up-front activities that assess critical areas and that take steps to mitigate information warfare threats to mission-critical system functions.

C. CONCLUSIONS

One key part of the modern RMA which is currently underway is the possibility of the development of a new form of warfare—often called information warfare. As part of an RMA, development of information warfare depends on technological changes, systems development and the adaptation of operational approaches and organizational structures in order to take advantage of this new capability. In the military, much of the focus has rightly been on assessing the doctrinal, operational and organizational issues of the information warfare revolution. But much less attention has been paid to the specific impacts of information warfare on technology research and acquisition activities. Thus the focus of this thesis is on assessing the nature of information warfare and the implications of the defining characteristics of information warfare for the research and acquisition systems. The underlying motivation is to ensure that the U.S. military is correctly postured to "win the IW RMA" by effectively researching, developing and acquiring information warfare capabilities.

In terms of the underlying nature of information warfare, it is clear there is not a textbook answer as to what information warfare does and does not encompass. Thus it is probably more useful to focus on what is new about information warfare as a starting point for assessing the impacts of information warfare. From this perspective, the most obvious characteristic is a dependence on information technology[7]—with most of these technologies either developed or available in the commercial world. This reliance on commercial

[7]It became hard to separate the acquisition of information warfare capabilities from the generic process of acquisition of information technology itself. Often the basic differentiating factor between acquiring information warfare capabilities and say, C4I capabilities, is the use to which the information technologies are applied. So many of the conclusions of this thesis deal with the broader subject of information technology acquisition and thus may apply to areas beyond the acquisition of information warfare systems or services.

technology is key and will be the driving force behind many of the changes required in military information technology research and acquisition. As information technology is popularized, standardized and commercialized, it becomes more and more difficult for the military to ignore the cost and quality benefits inherent in using products designed to compete in the free market.

Armed with the assumption that the bulk of information warfare technologies will come from the commercial sector, one must then tackle the question of what the centrally-managed military research and acquisition system should be doing. It seems clear there is still a role for the acquisition world, although it may be somewhat different from today. First, it should identify those areas where the business world is not likely to address military needs. This is the same type of activity already done for other technologies useful to the military. As an example, many aerospace technologies used by the military are widely available from commercial aerospace companies. But items like ejection seats and missile launchers are not standard commercial fare and so the military must provide the financial impetus for the development and acquisition of such products. The same is true for military-unique technologies useful in information warfare.

Second, the trend towards decentralization of information technology procurement should be vigorously pursued. With the development of commercial standards and a joint DoD-wide architecture that promotes interoperability and technology insertion, it is possible that skilled local users will be able to quickly procure and build systems to better meet their own needs. The acquisition community should not fight this trend in an attempt to keep control over standards, especially since the interoperability record of past centrally-procured systems has been less than spectacular. Nor should the issues of logistics support

necessarily be a barrier. With dependence on commercial technology, logistics may consist of discarding the "information appliance" and buying/leasing the newer version just put out by the business world. Instead the acquisition community should promote such decentralization by bringing its technological savvy to bear on the development of standards and architectures, by building easy-to-use contract vehicles for local warfighters to use, by providing systems integration expertise, by promoting new advances through incremental technology insertion and by concentrating on enhancing the underlying functions and services of systems. This last point bears further discussion. The more stable functions of information technology systems will largely be embodied in operational mission software. Based on the generic hardware and software available in the commercial arena, it is the mission software that truly makes a system a "military" system. Development and acquisition of this software is one of the most important activities for the acquisition community.

Finally, turning away from generic information technology acquisition topics, there is the specific issue of information protection during systems acquisition and development. Since dependence on commercial technology engenders an accompanying vulnerability to commercial technology, it is important to assess the risks posed by these vulnerabilities "upfront and early" in the development cycle. Methodologies already exist to perform such assessments as part of the engineering process—and these methodologies should be strengthened and their use expanded to all new or modified systems. In addition, concerns about product integrity because of software backdoors and "chipping" must be addressed. Since these problems are of interest to commercial firms as well, the military should seek to

engage much more closely with the traditionally non-defense firms who are providing much of the military's information infrastructure in order to deal with these concerns.

In sum, the defining characteristics of information warfare do prompt the need for changes in the acquisition community. These changes range from focusing R&D on military-unique technologies useful in information warfare to organizational modifications in information technology acquisition to adjustments and improvements in the acquisition process. Finally, in spite of any organization and operational adaptations made to accommodate information warfare, without changes in the realms of technology research and systems development, it is probable the U.S. military will not realize the full promise of information warfare.

LIST OF REFERENCES

Arquilla, John and Ronfeldt, David, "Cyberwar is Coming!" *Journal of Comparative Strategy*, Volume 12, no. 2, 1992.

Baker, Stewart, "Information Warfare and Encryption," electronic mail sent to Dave Farber, 23 April 1996.

Barnett, Jeff, Col., USAF, "The Revolution in Military Affairs," Office of Net Assessment briefing slides, undated.

Berkowitz, Bruce D., "Warfare in the Information Age," *Issues in Science and Technology*, Fall 1995.

Chairman of the Joint Chiefs of Staff (CJCS) Memorandum of Policy (MOP) 30, Command and Control Warfare, 8 March 1993.

Christian, Shelley, Major, USAF, et al., "Information Warfare: An Opportunity for Modern Warfare," Air Command and Staff College paper, 1 May 1995.

Crean, Tom, "Items of Potential Interest to Department of Defense Personnel—National Defense Authorization Act for FY 1996," information paper, 9 January 1996.

Daft, Richard L., *Organization Theory and Design*, St. Paul, MN: West Publishing Company, 1995.

DARPA Information Technology Office Homepage, URL: <http://www.ito.darpa.mil>, accessed 9 May 1996.

Drexler, K. Eric, *Unbounding the Future: The Nanotechnology Revolution,* New York: William Morrow and Company, Inc., 1991.

Dupont, Daniel G., "Smart Shopping—The Pentagon Tries to Teach Itself New Tricks," *Scientific American*, March 1996.

Emmett, Peter C., Squadron Leader, "Software Warfare: The Militarization of Logic," *Joint Force Quarterly*, Summer 1994.

"Evolutionary Acquisition Study," Armed Forces Communications and Electronics Association report, June 1993.

"Funding Innovation: Low-cost Options for Leveraging the Military Revolution," Defense Budget Project discussion paper, 11 April 1995.

"FY96 Implementation Plan," National Coordination Office for High Performance Computing and Communications, May 1995.

Giessler, Dr. Fred, "Reflexive Control, A Subsystem of Information Warfare," NDU briefing slides, July 1993.

"The Information Advantage," *Economist*, 10 June 1995.

"Information Architecture for the Battlefield," report of the Defense Science Board Summer Study Task Force, October 1994.

Information-Based Warfare Course slides, National Defense Univerity, March 1996.

Kraus, George F. Jr., "Information Warfare in 2015," *Proceedings*, August 1995.

Krepinevich, Andrew F., "Keeping pace with the Military-Technological Revolution," *Issues in Science & Technology*, Summer 1994.

Krepinevich, Andrew F., "Cavalry to Computer: The Pattern of Military Revolutions," *The National Interest*, Fall 1994.

Libicki, Martin C. & James A. Hazlett, "Do We Need an Information Corps?" *Joint Force Quarterly*, Autumn 1993.

Linstone, Harold A., *The Delphi Method*, Reading, MA: Addison-Wesley, 1975.

Loescher, Michael S., CDR, USN, "Selling Information Technology to the Navy in the Next Decade," text of a speech, undated.

Lynn, Larry, Acting Director, Advanced Research Projects Agency, "Prepared Statement before the Subcommittee on National Security, House Appropriations Committee," 23 March 1995.

Marshall, Andrew W., "RMA Update," Office of Net Assessment Memorandum for the Record, 2 May 1994.

"National Security Telecommunications Advisory Council (NSTAC) Fact Sheet," 2 January 1996.

"New World Vistas," report of the Air Force Scientific Advisory Board, 15 December 1995.

Nye, Joseph S. Jr. And Owens, William A., "America's Information Edge," *Foreign Affairs*, March/April 1996.

Paige, Emmett Jr., "Technical Architecture Framework for Information Management (TAFIM), Version 2.0," OASD(C3I) letter, 30 March 1995.

Pirog, John and Giordano, Joe, RL/IWT, interview conducted at Rome Lab on 16 April 1996.

Rosen, Stephen, *Winning the Next War —Innovation and the Modern Military*, Ithaca, HY: Cornell University Press, 1991.

Stoll, Clifford, *The Cuckoo's Egg*, New York: Doubleday, 1989.

Strassmann, Paul A., "Elements of and Information Management Doctrine for Low-Intensity Warfare," NDU paper, 20 January 1994.

Todd, Greg, "C[1] Catharsis," *Army*, February 1986.

BIBLIOGRAPHY

"Acquiring Defense Software Commercially," report of the Defense Science Board Task Force, June 1994.

Adam, John A., "Warfare in the Information Age," *IEEE Spectrum*, September 1991.

Air Force Information Warfare Center, "Air Force Information Warfare Center," undated briefing slides.

Allard, Kenneth, Col., USA, "Data Transforms Warfare," *Defense News*, 4 March 1996.

Allard, Kenneth, Col., USA, interview conducted at the Naval Postgraduate School, 8 March 1996.

Andrews, Duane P. And Knecht, Ronald J., "Improving the Security of Information in DoD," 8 March 1994.

Army Digitization Office, "Providing the Means," undated pamphlet.

Arnett, Eric H., "Welcome to Hyperwar," *The Bulletin of the Atomic Scientists*, September 1992.

Arquilla, John and Ronfeldt, David, "Cyberwar is Coming!" *Journal of Comparative Strategy*, Volume 12, no. 2, 1992.

Arquilla, John, "Strategic Implications of Information Dominance," *Strategic Review*, Summer 1994.

Arquilla, John, "Warfare in the Information Age," briefing slides for a presentation to the DoE Information Warfare Conference, 23 August 1995.

Ayers, Robert L., "DISA and Information Warfare," undated briefing slides.

Baker, Stewart, "Information Warfare and Encryption," electronic mail sent to Dave Farber, 23 April 1996.

Bankes, Steve, and Builder, Carl, "Seizing the Moment: Harnessing the Information Technologies," *The Information Society*, Vol. 8, No. 1, 1992.

Barnett, Jeff, Col., USAF, "The Revolution in Military Affairs," Office of Net Assessment briefing slides, undated.

Barnett, Jeff, Col., USAF, "The Revolution in Military Affairs," Office of Net Assessment fact sheet, December 1995.

Beniger, James, *The Control Revolution*, Cambridge, MA: Harvard University Press, 1986.

Benedickt, Michael, *Cyberspace - First Steps*, MIT Press, Cambridge, 1991.

Berenson, Dr. Paul J., "Knowledge Based Warfare," TRADOC briefing slides, December 1995.

Berkowitz, Bruce D., "Warfare in the Information Age," *Issues in Science and Technology*, Fall 1995.

Berry, F. Clifton, Jr., *Inventing the future: How science and technology transform our world*, Brassey's Inc., McClean, VA, 1993.

Bunker, Robert J., "Transition to fourth epoch war," *Marine Corps Gazette*, September 1994.

Burnette, Gerald, LCDR, USN, "Information, The Battlefield of the Future," *Surface Warfare*, July/August 1995.

Canavan, Gregory, "Simulation, Computing, Information and Future Warfare," Los Alamos National Laboratory, LA-12490-MS, 1990.

Campen, Alan D., ed., *The First Information War*, Fairfax, VA: AFCEA International Press, October 1992.

Campen, Alan D., "Rush to Information-Based Warfare Gambles with National Security," *Signal*, July 1995.

Campen, Alan D., "Rush to Information-Based Warfare Gambles with National Security," briefing slides, December 1995.

Chairman of the Joint Chiefs of Staff (CJCS) Memorandum of Policy (MOP) 30, *Command and Control Warfare*, 8 March 1993.

Christian, Shelley, Major, USAF, et al., "Information Warfare: An Opportunity for Modern Warfare," Air Command and Staff College paper, 1 May 1995.

Clapper, James R., Lt. Gen., USAF, and Trevino, Eben H., Lt. Col., USAF, "New Objectives, Strategies Needed to Optimize Information Warfare," *Signal*, March 1995.

Clark, Howard W. And Wallfesh, Saundra K., "Measuring Effectiveness of Theater IW/C2W Campaigns," unpublished Dynamics Research Corporation paper, April 1995.

Cohen, Eliot A., "A Revolution in Warfare," *Foreign Affairs*, March/April 1996.

Cook, W. C., "Information Warfare: A New Dimension in the Application of Air and Space Power," Air War College, April 1993.

Cooper, Pat & Oliveri, Frank, "Air Force Carves Operational Edge in Info Warfare," *Defense News*, 21-27 August 1995.

Cooper, Jeffrey R., "Another View of the Revolution in Military Affairs," SRS Technologies white paper, March 1994.

Cooper, Jeffrey R., "Applying Information Technologies to Low Intensity Conflict: 'Real-Time Information Shield' Concept," SRS Technologies White Paper, December 1992.

Cooper, Jeffrey R., "Dominant Battlespace Awareness: Implications for the Future Conduct of Warfare," SRS Technologies white paper, December 1994.

Cooper, Jeffrey R., "The Coherent Battlefield–Removing the 'Fog of War': A Framework for Understanding an MTR of the 'Information Age,'" SRS Technologies white paper, June 1993.

Cooper, Jeffrey R., "Towards a Theory of Coherent Operations," SRS Technologies white paper, June 1994.

"Cornerstones of Information Warfare," United States Air Force white paper.

Crean, Tom, "Items of Potential Interest to Department of Defense Personnel—National Defense Authorization Act for FY 1996," information paper, 9 January 1996.

Daft, Richard L., *Organization Theory and Design*, St. Paul, MN: West Publishing Company, 1995.

DARPA Information Technology Office Homepage, URL: <http://www.ito.darpa.mil>, accessed 9 May 1996.

"Data Security, Special Report," *IEEE Spectrum*, August 1992.

De Caro, Chuck, "Sats, Lies, and Video-rape: The Soft War Handbook," undated paper.

DeLanda, Manuel, *War in the Age of the Intelligent Machines*, New York: Zone Books, 1991.

"Defensive Information Warfare," Joint Staff/J6 briefing slides, December 1995.

Devost, Matthew G., "National Security in the Information Age," University of Vermont Thesis, May 1995.

Downs, Lawrence G., CDR, USN, "Digital Data Warfare: Using Malicious Computer Code as a Weapon," Air War College paper, April 1995.

Dretske, Fred., *Knowledge and the Flow of Information*, Cambridge, MA: MIT Press, 1981.

Drexler, K. Eric, *Unbounding the Future: The Nanotechnology Revolution*, New York: William Morrow and Company, Inc., 1991.

Dunlap, Charles F. Jr., "A Warning from the Future, How we Lost the High-Tech War of 2007," *The Weekly Standard*, 29 January, 1996.

Dunn, Richard J. III, "From Gettysburg to the Gulf and Beyond: Coping with Revolutionary Technological Change in Land Warfare," McNair Papers, Number Thirteen, Institute for National Strategic Studies.

Dupont, Daniel G., "Smart Shopping—The Pentagon Tries to Teach Itself New Tricks," *Scientific American*, March 1996.

Elam, Donald, LT, USN, et al., "Information Warfare: A Revolution in Modern Warfighting Concepts," unpublished paper prepared for EO 3802, Electronic Warfare Computer Applications, Naval Postgraduate School, June 1995.

Elliot, Ronald D. & Bradley, Scott, Major, USMCR, "Effective Command and Control: Affordable Revolutionary Opportunities to Improve Modern Defense Capabilities," undated.

Emmett, Peter C., Squadron Leader, "Software Warfare: The Militarization of Logic," *Joint Force Quarterly*, Summer 1994.

"Evolutionary Acquisition Study," Armed Forces Communications and Electronics Association report, June 1993.

FitzGerald, Mary C., "Russian Views on Information Warfare," *Army*, Vol. 44, No. 5, May 1994.

FitzSimonds, CAPT James R., USN, "The Revolution in Military Affairs: Challenges for Defense Intelligence," OSD Net Assessment briefing slides, undated.

FM 100-6 (draft), *Information Operations*, 22 July 1994.

Fogleman, General Ronald R., USAF, "Fundamentals of Information Warfare—An Airman's View," Air Force Update 95-09, June 1995.

Fogleman, General Ronald R., USAF, "Getting the Air Force into the 21st Century," text of an address presented to the Air Force Association's Air Warfare Symposium, Orlando, FL, 24 February 1995.

Fogleman, General Ronald R.,USAF, "Information Operations: The Fifth Dimension of War," *Defense Issues*, Volume 10, Number 47.

Fogleman, General Ronald R., USAF, "Quotable Quotes," Air Force Update 95-10, June 1995.

Forester, Tom, *The Information Technology Revolution*, Cambridge, MA: The MIT Press, 1985.

Frank, Dr. Howard, Director, "National Information Infrastructure Challenges and Opportunities," ARPA/DISA Advanced Information Technology Services briefing slides, undated.

Frankel, Dr. Michael S., "The 1994 Army Science Board Recommended Technical Architecture for the Digital Battlefield," *Army Research, Development and Acquisition Bulletin*, November-December 1994.

Frizzelle, Major Charles, USAF, OSD/CISA, "Feedback On Question," electronic mail sent to Capt Roger Thrasher, 29 Mar 1996.

"FY96 Implementation Plan," National Coordination Office for High Performance Computing and Communications, May 1995.

"Funding Innovation: Low-cost Options for Leveraging the Military Revolution," Defense Budget Project discussion paper, 11 April 1995.

Garigue, Robert., "Information Warfare Concepts," Draft 2.0, DSIS DND Government of Canada, 1995.

Gelernter, David, *Mirror Worlds, or the Day Software Puts the Universe in a Shoebox...How It Will Happen and What It Will Mean*, New York: Oxford University Press, 1991.

Giessler, Dr. Fred, "Competing Cybernetic Systems, A Scientific Construct for Information Warfare," SAIC briefing slides, October 1994.

Giessler, Dr. Fred, "Reflexive Control, A Subsystem of Information Warfare," NDU briefing slides, July 1993.

Gingrich, Newt, "Information Warfare: Definition, Doctrine and Direction," text of a speech to Information Resources Management College, National Defense University, 3 May 1994.

Gingrich, Newt, "Information Warfare," text of a speech to AFCEA conference, Hyatt Regency Crystal City, 8 February 1995.

"Global Presence 1995," United States Air Force white paper, 1995.

Grier, Peter, "Information Warfare," *Air Force*, March 1995.

Griffith, Major Thomas E., Jr., USAF, "Strategic Attack of National Electrical Systems," School of Advanced Airpower Studies paper, Air University, October 1994.

Hammes, Thomas X., Lt. Col., USMC, "Evolution of war: The fourth generation," *Marine Corps Gazette*, September 1994.

Hazlett, James A., CDR, USN, "'Just-In-Time' Warfare—Designing a Reconnaissance-Strike-Defense Complex (RSDC)," National Defense University unpublished paper.

Hazlett, James A., CDR, USN, "'Just-In-Time' Warfare," unpublished paper.

"High Performance Computing and Communications: Foundation for America's Information Future, Supplement to the President's FY 1996 Budget," National Science and Technology Council, 1995.

Holley, I.B., *Ideas and Weapons*, Yale University Press, 1953.

Hughes, Wayne P., "Command and Control Within the Framework of a Theory of Combat," Naval Postgraduate School, undated.

Hurska, Jan, *Computer Viruses and Anti-Virus Warfare*, New York: Ellis Horwood Publishers, 1990.

Hust, Major Gerald R., "Taking Down Telecommunications," Air University paper, 1994.

Hutcherson, N. B., Lt. Col., USAF "Command and Control Warfare—Putting Another Tool in the War-Fighter's Data Base," Air University paper, September 1994.

"The Information Advantage," *Economist*, 10 June 1995.

"Information Architecture for the Battlefield," report of the Defense Science Board Summer Study Task Force, October 1994.

Information-Based Warfare Course slides, National Defense Univerity, March 1996.

"Information Power: A Framework for Action," GRC Concept Paper, undated.

"Information Warfare: Pouring the Foundation," United States Air Force white paper (draft), 19 December 1994.

"Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance," research report prepared for Chief, Information Warfare Division (J6K), 4 July 1995.

Jensen, Owen E., Col., USAF, "Information Warfare: Principles of Third-wave War," *Airpower Journal*, Winter 1994.

Joint Publication 3-13 (draft), *Joint Doctrine for Command and Control Warfare (C^2W): Battlefield Application of Information Warfare*, March 1995.

Johnson, Stuart E. & Libicki, Martin C., editors, *Dominant Battlespace Knowledge: The Winning Edge*, National Defense University Press, Washington DC, 1995.

"Jumpstart, Information Warfare: An Introduction," Air University Center for Aerospace Doctrine, Research and Education (CADRE) briefing, undated.

King, Roy M., Lt. Col., USAF, "Achieving Information Dominance Through Information Warfare," Air War College paper, April 1995.

Knect, Ron, "Information Dependency," briefing slides, 27 June 1995.

Komar, David M., Lt. Col., USAF, "Information-Based Warfare: A Third Wave Perspective," Air War College paper, May 1995.

Kraus, George F. Jr., "Information Warfare in 2015," *Proceedings*, August 1995.

Kraus, George F. Jr., "Information Warfare: Russian Views," briefing slides, September 1995.

Krepinevich, Andrew F., "Keeping pace with the Military-Technological Revolution," *Issues in Science & Technology*, Summer 1994.

Krepinevich, Andrew F., "Cavalry to Computer: The Pattern of Military Revolutions," *The National Interest*, Fall 1994.

Kuehl, Dr. Dan, "Target Sets for Strategic Information Warfare in an Era of Comprehensive Situational Awareness," unpublished paper, 24 January 1995.

Lewonowski, M.C., "Information War," Air War College paper, 1991.

Libicki, Martin C., *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon*, Washington, DC: National Defense University Press, 1994.

Libicki, Martin C., "What is Information Warfare?" *Strategic Forum*, May 1995.

Libicki, Martin C., *What is Information Warfare?,* Washington, DC: National Defense University Press, August 1995.

Libicki, Martin C. & James A. Hazlett, "Do We Need an Information Corps?" *Joint Force Quarterly*, Autumn 1993.

Libicki, Martin C. & James A. Hazlett, "The Revolution in Military Affairs" *Strategic Forum*, November 1994.

Linstone, Harold A., *The Delphi Method*, Reading, MA: Addison-Wesley, 1975.

Loescher, Michael S., CDR. USN, "The Croesus Strategies: New Approaches to Fielding Information Systems Technologies," June 1992.

Loescher, Michael S., CDR. USN, interview conducted on 28 March 1996.

Loescher, Michael S., CDR. USN, "Selling Information Technology to the Navy in the Next Decade," text of a speech, undated.

Luoma, William M., "Netwar: The Other Side of Information Warfare," Naval War College thesis, February 1994.

Lynn, Larry, Acting Director, Advanced Research Projects Agency, "Prepared Statement before the Subcommittee on National Security, House Appropriations Committee," 23 March 1995.

Mann, Edward, "Desert Storm: The First Information War?," *Airpower Journal*, VIII No. 4, Winter 1994.

Marshall, Andrew W., "The Military-Technical Revolution: Apreliminary Assessment," Office of Net Assessment Memorandum for the Record, 9 September 1992.

Marshall, Andrew W., "RMA Update," Office of Net Assessment Memorandum for the Record, 2 May 1994.

Marshall, Andrew W., "Some Thoughts on Military Revolutions—Second Version," Office of Net Assessment Memorandum for the Record, 23 August 1993.

Mazarr, Michael, et al., "The Military Technical Revolution: a structural framework," Centre for Strategic and International Studies, 1993.

McCarthy, Michael, Capt., USAF, HQ USAF/INXI, interview conducted on 28 March 1996.

McCorry, Daniel C. Jr., Lt. Col., USAF, "Third Wave Military Acquisition: Organizational & Management Considerations for a Complex System," Naval War College thesis, 16 June 1995.

Minihan, Kenneth A., Major General, USAF, "Information Dominance: Meeting the Intelligence Needs of the 21st Century," *American Intelligence Journal,* Spring/Summer 1994.

Morris, Chris, Morris, Janet, and Baines, Thomas, "Weapons of Mass Protection: Nonlethality, Information Warfare, and Airpower in the Age of Chaos," *Airpower Journal,* Spring 1995.

Munro, Neil, *The Quick and the Dead*, New York: St. Martin's Press, 1991.

Nair, V.K., *War in the Gulf: Lessons for the Third World*, New Delhi, India: Lancer International, 1991.

"National Security Telecommunications Advisory Council (NSTAC) Fact Sheet," 2 January 1996.

Nelson, Andrew H., *The Art of Information War*, 1995.

"New World Vistas," report of the Air Force Scientific Advisory Board, 15 December 1995.

Nye, Joseph S. Jr. And Owens, William A., "America's Information Edge," *Foreign Affairs*, March/April 1996.

Paige, Emmett Jr., "Technical Architecture Framework for Information Management (TAFIM), Version 2.0," OASD(C3I) letter, 30 March 1995.

Peterson, John, *The Road to 2015: Profiles of the Future*, Waite Group Press, 1994.

Pirog, John and Giordano, Joe, RL/IWT, interview conducted at Rome Lab on 16 April 1996.

Probst, David K., "The United States Needs a Scalable Shared-Memory Multiprocessor, But Might Not Get One!" NCO White Paper, 6 June 1995.

Rigby, Joe W., Major General, USA, "Acquiring the Digitized Force," *International Defense Review*, November 1995.

Rigby, Joe W., Major General, USA, "Battlefield Digitization: When the Talking has to Stop," *Army Research, Development and Acquisition Bulletin*, November-December 1994.

Rona, Thomas P., "The Case for Metadiversity," unpublished paper, September 1995.

Rona, Thomas P., "Weapons Systems and Information War," draft paper, July 1976.

Rosen, Stephen, *Winning the Next War —Innovation and the Modern Military,* Ithaca, HY: Cornell University Press, 1991.

Rothrock, John, "Information Warfare: Time for Some Constructive Skepticism?," *American Intelligence Journal*, Spring/Summer 1994.

Rowe, Wayne, "Information Warfare: A Primer for Navy Personnel," Naval War College paper, 23 June 1995.

Rowell, Michael O., Major, USMC, "Animal Crackers: Weakness in our C4I Strengths," Naval War College, 13 February 1995.

Ryan, Lt. Col. Donald E., Jr., USAF, "Implications of Information-Based Warfare," *Joint Force Quarterly*, Autumn-Winter 1994-1995.

Schwartau, Winn, *Information Warfare: Chaos on the Electronic Superhighway*, New York: Thunders Mouth Press, 1994.

Science Application International Corporation (SAIC), "Planning Considerations for Defensive Information Warfare—Information Assurance", 16 December 1993.

Scott, William B., "'Information Warfare' Demands New Approach," *Aviation Week & Space Technology*, 13 March 1995.

Skukman, David, *The Sorcerer's Challenge: Fears and Hopes for the Weapons of the Next Millennium*, London: Hodder & Stoughton, 1995.

Smith, K.B., "Crisis and Opportunity of Information War," Army Command and General Staff College thesis, 6 May 1994.

Smyth, Joseph S., Major, USAF, et al., "CONOPS 2010, Section 1, Information Dominance 2010 (INFODOM 2010)," Air Command and Staff College research paper, May 1995.

"The Softwar Revolution: The Ties that Bind," *Economist*, 10 June 1995.

"Special Report on Information Warfare," *Computer Security Journal*, Fall 1995.

Steele, Robert D., "The Military Perspective on Information Warfare: Apocalypse Now", Keynote Speech to Second International Conference on Information Warfare, 19 January 1995.

Steele, Robert D., "The Transformation of War and the Future of the Corps", 28 April 1992.

Steele, Robert D., "War and Peace in the Age of Information (Text)," text of a Superintendent's Guest Lecture, Naval Postgraduate School, 17 August 1993.

Stein, George J., "Information Warfare," *Airpower Journal*, Spring 1995.

Stewart, John F., Major General, USA, "Command and Control Warfare and Intelligence on the Future Digital Battlefield," *Army Research, Development and Acquisition Bulletin*, November-December 1994.

Stoll, Clifford, *The Cuckoo's Egg*, New York: Doubleday, 1989.

"Strategic Implementation Plan: America in the Age of Information," National Coordination Office for High Performance Computing and Communications, 10 March 1995.

Strassmann, Paul A., "Selected Topics on Information Terrorism," briefing slides, 15 December 1995.

Strassmann, Paul A., "Elements of and Information Management Doctrine for Low-Intensity Warfare," NDU paper, 20 January 1994.

Sullivan, Gordon R., General, USA, "Force XXI: Digitizing the Battlefield," *Army Research, Development and Acquisition Bulletin*, November-December 1994.

Szafranski, Richard, "A Theory of Information Warfare: Preparing for 2020," *Airpower Journal*, Spring 1995.

Thompson, Mark, "If War Comes Home," *Time*, 21 August 1995.

Todd, Greg, "C[1] Catharsis," *Army*, February 1986.

Toffler, Alvin, *Powershift: Knowledge, Wealth, and Violence at the Edge of the 21st Century*, New York: Bantam Books, 1990.

Toffler, Alvin and Heidi, *War and Anti-War: Survival at the dawn of the 21st Century*, New York: Little and Brown, 1993.

TRADOC Pamphlet 525-5, *Force XXI Operations*, 1 August 1994.

TRADOC Pamphlet 525-29, *Concept for Information Operations*, 1 August 1995.

Van Creveld, Martin, *Command in War*, Cambridge: Harvard Press, 1985.

Van Creveld, Martin, *Technology and War: From 2000 B.C. to the Present*, New York: The Free Press, 1989.

Van Creveld, Martin, *The Transformation of War*, New York: Free Press, 1991.

Vickers, Michael G, "A Concept for Theater Warfare in 2020," Office of Net Assessment paper, 1993.

Waller, Douglas, "Onward Cyber Soldiers," *Time*, 21 August 1995.

"Warfighting Vision 2010, A Framework for Change," Joint Warfighting Center draft paper, 11 September 1995.

Watters, Jim, et al., "IW System Assessment—Process and Highlights," briefing slides, undated.

Wilcox, Greg, "Information Warfare" SRI International briefing slides, 2-4 December 1993.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Rd., STE 0944
   Alexandria, Virginia 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Rd.
   Monterey, California 93943-5101

3. INSS 2
   USAFA/DFE
   2354 Fairchild Dr., Suite 5D33
   USAF Academy, CA 80840

4. AFIT Library 1
   WPAFB, OH 45433

5. USAFA Library 1
   USAF Academy, CO 80840

6. Professor Carl R. Jones, SM/Js 1
   Department of Systems Management
   Naval Postgraduate School
   Monterey, CA 93943-5103

7. Professor Dan C. Boger, CC 2
   C3 Academic Group
   Naval Postgraduate School
   Monterey, CA 93943-5000

8. LTC Ernest K. Beran 1
   Code 39
   Naval Postgraduate School
   Monterey, CA 93943-5000

9. USAF/AQI 1
   Air Force Pentagon
   Washington, DC 20330

10. Col Ken Allard 1
    National Defense University, Ft McNair
    Washington, DC 20319

11. Col (Ret.) Alan Campen 1
14305 Shelter Cove Road
Midlothian, VA 23112

12. VADM Arthur Cebrowski 1
JCS/J6
6000 Pentagon
Washington, DC 20318-6000

13. Major George Cho 1
ESC/ICW
Hanscom AFB, MA 01731

14. Peter Cochrane 1
Head of Advanced Research
BT Laboratories (Admin 3)
Martlesham Heath
IPSWICH IP5 7RE
UK

15. Fred Cohen 1
PO Box 1480
Hudson, OH 44236

16. Matthew Devost 1
7812 Butterfield Lane
Annandale, VA 22003

17. AFIT/CI 2
2950 P St., Bldg 125
Wright-Patterson AFB, OH 45433

18. LT Don Elam 1
85 Redwood Drive
Stanton, KY 40380

19. LCDR (N) Robert Garigue 1
NDHQ
Mgen Pearke Bld
Ottawa, K1A OK2
Canada

20. Fred Giessler 2
National Defense University, Ft McNair
Washington, DC 20319

21. Joe Giordano/John Pirog 2
RL/IWT
525 Brooks Road
Rome, NY 13441-4505

22. LTC Paul Gregory 1
CINCUSACOM/J362
1562 Mitscher Avenue, Suite 200
Norfolk, VA 23551

23. BG David Gust 1
SFAE-IEW
Ft Monmouth, NJ 07703

24. James Hazlett 1
SAIC
1710 Goodridge Drive, M/S T1-5-3
McLean, VA 22102

25. John Howard 1
Dept Of EPP, Baker Hall 129
Carnegie Mellon University
Pittsburgh, PA 15213

26. Ken King 1
Digital Equipment Corporation
30 Porter Road, LJO2/E4
Littleton, MA 01460-1446

27. Ronald Knect 1
SAIC
1710 Goodbridge Drive, M/S 1-14-9
McLean, VA 22102-3799

28. Professor Fred Levien, CC 1
Information Warfare Academic Group
Naval Postgraduate School
Monterey, CA 93943-5000

29. Martin Libicki 1
National Defense University, Ft McNair
Washington, DC 20319

30. Maj Gen Robert Linhard 1
1480 Air Force Pentagon 4E1046
Washington DC 20330-1480

31. CDR Michael Loescher 1
Crystal Plaza 6, Rm 780
2401 North Glebe Road
Arlington, VA 22207

32. Col Robert Maynard 1
AFIWC/SC
102 Hall Blvd, Suite 316
San Antonio, TX 78243-7021

33. Captain Michael McCarthy 2
USAF/INXI, Room 4C110
1700 Air Force Pentagon
Washington, DC 20330-1700

34. Larry Merritt 1
AFIWC/CA
102 Hall Blvd, Suite 345
San Antonio, TX 78243-7038

35. Dr David Probst 1
Concordia University, Department Of Computer Science
1455 De Maisonneuve West
Montreal QUEBEC H3G 1M8
Canada

36. John Regnault 1
BT Laboratories (Admin 2)
Martlesham Heath
IPSWICH IP5 7RE
UK

37. David Ronfeldt 1
1700 Main St.
Santa Monica, CA 90406

38. G. L. Ruptier 1
NCCOSC RDTE DIV 0207
53570 Silvergate Ave
San Diego, CA 92152-5001

39. Major Donna Schutzius 1
2354 Fairchild Dr., Suite 6A26
USAF Academy, CO 80840

40. Winn Schwartau 1
11511 Pine St.
Seminole, FL 34642

41. Robert Steele 1
11005 Langton Arms Court
Oakton, VA 22124-1807

42. Capt Roger Thrasher 20
49 Carlisle Road
Transfer, PA 16154

43. Col David Todd 2
USAF/XOXT
1480 Air Force Pentagon
Washington DC 20330-1480

44. LTC Andy Weaver 1
609th IWS
Shaw AFB, SC 29152